CISCO ™

Firepower 8000 Series Hardware Installation Guide

First Published: July 22, 2016
Last Updated: July 12, 2018

CONTENTS

About This Guide

Updated: July 22, 2016

This guide describes how to install and maintain the Cisco Firepower 8000 Series appliances. Information in this guide applies to the Cisco 80xx Family, 81xx Family, and the 83xx Family models.

This preface includes the following sections:

Organization

This guide is organized as follows:

Chapter	Title	Description
Chapter 1	About the Firepower 8000 Series	Provides an overview of the devices included in the 8000 Series.
Chapter 2	Hardware Specifications	Describes the hardware specifications for the Firepower 8000 Series models.
Chapter 3	Installing a Firepower 8000 Series Device	Describes how to install a Firepower 8000 Series device in a rack, how to connect the management interface, and how to power on the chassis.
Chapter 4	Using the LCD Panel on a Firepower Device	Describes how to view device information or configure certain settings using an LCD panel on the front of the device instead of the system's web interface.
Chapter 5	Deploying on a Management Network	Describes Firepower System deployment options available to accommodate the needs of unique network architectures.

Chapter	Title	Description
Chapter 6	Deploying Firepower Managed Devices	Describes how different sensing interfaces affect the capabilities of the Firepower System, including passive, inline, routed, switched, and hybrid interfaces.
Appendix A	Power Requirements for Firepower 8000 Series Devices	Describes AC and DC power requirements for Firepower 8000 Series devices.
Appendix B	Inserting and Removing Firepower 8000 Series Modules	Describes how to insert a new module or how to remove or replace a preinstalled module in Firepower 8000 Series devices.
Appendix C	Installing a Malware Storage Pack	Describes how to install a malware storage pack in Firepower 8000 Series devices.

Document Conventions

This document uses the following conventions:

Convention	Indication
bold type	Commands and keywords and user-entered text appear in **bold** type.
italic type	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* type.
[ ]	Elements in square brackets are optional.
{x	y	z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x	y	z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	An unquoted set of characters. Do not use quotation marks around the string, or the string will include the quotation marks.
monospace type	Terminal sessions and information the system displays appear in monospace type.
monospace bold type	Commands and keywords and user-entered text appear in **monospace courier** type.
monospace italic type	Arguments for which you supply values are in *monospace italic* type.
< >	Non-printing characters such as passwords are presented in angle brackets.
[ ]	Default responses to system prompts are presented in square brackets.
!, #	An exclamation point (!) or a hash sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*.

Tip Means *the following information will help you solve a problem.*

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Installation Warnings

Be sure to read the Regulatory Compliance and Safety Information document (http://www.cisco.com/c/en/us/td/docs/security/firesight/hw-docs/regulatory/compliance/firesight-firepower-rcsi.html) before installing the device.

This section presents these important safety warnings:

- Power Supply Disconnection Warning, page vii
- Jewelry Removal Warning, page vii
- Wrist Strap Warning, page viii
- Work During Lightning Warning, page viii
- Installation Instructions Warning, page viii
- Chassis Warning for Rack-Mounting and Servicing, page viii
- Short-Circuit Protection Warning, page viii
- SELV Circuit Warning, page viii
- Ground Conductor Warning, page viii
- Faceplates and Cover Panels Warning, page ix
- Product Disposal Warning, page ix
- Compliance with Local and National Electrical Codes Warning, page ix
- Grounded Equipment Warning, page ix
- Safety Cover Requirement, page ix

Power Supply Disconnection Warning

Warning **Before working on a chassis or working near power supplies, unplug the power cord on AC units; disconnect the power at the circuit breaker on DC units.** Statement 12

Jewelry Removal Warning

Warning **Before working on equipment that is connected to a power source, remove jewelry (including rings, necklaces, and watches). Metal objects will heat when connected to power and ground, and can cause serious burns or weld the metal object to the terminals.** Statement 43

Wrist Strap Warning

⚠

Warning **During this procedure, wear grounding wrist straps to avoid ESD damage to the card. Do not directly touch the backplane with your hand or any metal tool, or you could receive a shock.** Statement 94

Work During Lightning Warning

⚠

Warning **Do not work on the system, or connect or disconnect cables during periods of lightning. Statement 1001**

Installation Instructions Warning

⚠

Warning **Read all installation instructions before connecting the system to a power source.** Statement 1004

Chassis Warning for Rack-Mounting and Servicing

⚠

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety: This unit should be mounted at the bottom of the rack if it is the only unit in the rack. When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.** Statement 1006

Short-Circuit Protection Warning

⚠

Warning **This product requires short-circuit (overcurrent) protection, to be provided as part of the building installation. Install only in accordance with national and local wiring regulations.** Statement 1045

SELV Circuit Warning

To avoid electric shock, do not connect safety extra-low voltage (SELV) circuits to telephone-network voltage (TNV) circuits. LAN ports contain SELV circuits, and WAN ports contain TNV circuits. Some LAN and WAN ports both use RJ-45 connectors. Use caution when connecting cables. Statement 1021

Ground Conductor Warning

⚠

Warning **This equipment must be grounded. Never defeat the ground conductor, or operate the equipment in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority, or an electrician if you are not certain that suitable grounding is available.** Statement 1024

Faceplates and Cover Panels Warning

Warning **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they restrict electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.** Statements 1029 and 142

Product Disposal Warning

Warning **Ultimate disposal of this product should be handled according to all national laws and regulations.** Statement 1040

Compliance with Local and National Electrical Codes Warning

Warning **Installation of the equipment must comply with local and national electrical codes.** Statement 1074

Grounded Equipment Warning

Warning **This equipment is intended to be grounded. Ensure that the host is connected to earth ground during normal use.** Statement 39

Safety Cover Requirement

Warning **The safety cover is an integral part of the product. Do not operate the unit without the safety cover installed. Operating the unit without the cover in place will invalidate the safety approvals and pose a risk of fire and electrical hazards.** Statement 117

Where to Find Safety and Warning Information

For safety and warning information, see the Regulatory Compliance and Safety Information document at the following URL:

http://www.cisco.com/c/en/us/td/docs/security/firesight/hw-docs/regulatory/compliance/firesight-firepower-rcsi.html

This RCSI document describes the international agency compliance and safety information for the Cisco Firepower series.

Related Documentation

For a complete list of the Cisco Firepower series documentation and where to find it, see the documentation roadmap at the following URL:

http://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

About the Firepower 8000 Series

This chapter describes the Cisco Firepower 8000 Series devices, which are fault-tolerant, purpose-built network appliances available with a range of throughputs and capabilities.

Devices deployed on network segments within your organization monitor traffic for analysis. Devices deployed passively help you gain insight into your network traffic. Deployed inline, you can use Firepower devices to affect the flow of traffic based on multiple criteria.

You **must** manage Firepower 8000 Series devices with a Firepower Management Center.

Warning **Only trained and qualified personnel should install, replace, or service this equipment.** Statement 49

Firepower 8000 Series Managed Devices Delivered with Firepower System

The following table lists the Firepower 8000 Series managed devices that Cisco delivers with the Firepower System.

Table 1-1 *Firepower 8000 Series Appliances*

Models/Family	Series/Grouping	Type
80xx Family: • AMP8050	8000 Series	device
81xx Family: • 8120, 8130, 8140 • AMP8150	8000 Series	device
82xx Family: • 8250 • 8260, 8270, 8290	8000 Series	device
83xx Family: • 8350 • 8360, 8370, 8390 • AMP8350 • AMP8360, AMP8370, AMP8390	8000 Series	device

Firepower 8000 Series Device Chassis Designations

The following table lists the chassis designations for the Firepower 8000 Series models available world-wide. The chassis code appears on the regulatory label on the outside of the chassis, and is the official reference code for hardware certifications and safety.

Table 1-2   8000 Series Chassis Models

Firepower and AMP Device Model	Hardware Chassis Code
AMP8050 (AC or DC power)	CHAS-1U-AC/DC
8120, 8130, 8140, AMP8150 (AC or DC power)	CHAS-1U-AC/DC
8250, 8260, 8270, 8290 (AC or DC power)	CHAS-2U-AC/DC
8350, 8360, 8370, 8390 (AC or DC power)	PG35-2U-AC/DC
AMP830, AMP8360, AMP8370, AMP8390 (AC or DC power)	PG35-2U-AC/DC

Hardware Specifications

Firepower 8000 Series devices are delivered on a variety of platforms to meet the needs of your organization.

Rack and Cabinet Mounting Options

You can mount Firepower devices in racks and server cabinets. The appliance comes with a rack-mounting kit. For information on mounting the appliance in a rack, refer to the instructions delivered with the rack-mounting kit.

Firepower 8000 Series Devices

The Firepower 8000 Series devices use network modules (NetMods) that contain either copper or fiber sensing interfaces. The devices can be shipped fully assembled or you can install the modules. Assemble your device before installing the Firepower System. See the assembly instructions shipped with your modules.

Some 8000 Series devices can be stacked to increase the capability of the system. For each stacking kit, you replace a NetMod with a stacking module and cable the devices together using the 8000 Series stacking cable. See Using Devices in a Stacked Configuration, page 3-10 for more information.

The Firepower 8000 Series device can be delivered on a variety of chassis:

- AMP8050 is a 1U chassis and can contain up to three modules.

- Firepower 8120, 8130, 8140, and AMP8150, also known as the 81xx Family, is a 1U chassis and can contain up to three modules. For the Firepower 8140 only, you can add a stacking kit for a total 2U configuration.

- Firepower 8250, part of the 82xx Family, is a 2U chassis and can contain up to seven modules. You can add up to three stacking kits for a total 8U configuration.

- Firepower 8260, part of the 82xx Family, is a 4U configuration with two 2U chassis. The primary chassis contains one stacking module and up to six sensing modules. The secondary chassis contains one stacking module. You can add up to two stacking kits for a total 8U configuration.

- Firepower 8270, part of the 82xx Family, is a 6U configuration with three 2U chassis. The primary chassis contains two stacking modules and up to five sensing modules. Each secondary chassis contains one stacking module. You can add one stacking kit for a total 8U configuration.

- Firepower 8290, part of the 82xx Family, is an 8U configuration with four 2U chassis. The primary chassis contains three stacking modules and up to four sensing modules. Each secondary chassis contains one stacking module. This model is fully configured and does not accept a stacking kit.

- Firepower 8350 and AMP8350, part of the 83xx Family, is a 2U chassis and can contain up to seven modules. You can add up to three stacking kits for a total 8U configuration.

- Firepower 8360 and AMP8360, part of the 83xx Family, is a 4U configuration with two 2U chassis. The primary chassis contains one stacking module and up to six sensing modules. The secondary chassis contains one stacking module. You can add up to two stacking kits for a total 8U configuration.

- Firepower 8370 and AMP8370, part of the 83xx Family, is a 6U configuration with three 2U chassis. The primary chassis contains two stacking modules and up to five sensing modules. Each secondary chassis contains one stacking module. You can add one stacking kit for a total 8U configuration.

- Firepower 8390 and AMP8390, part of the 83xx Family, is an 8U configuration with four 2U chassis. The primary chassis contains three stacking modules and up to four sensing modules. Each secondary chassis contains one stacking module. This model is fully configured and does not accept a stacking kit.

Note The AMP models have many of the same form factors as their Firepower counterparts, but have been optimized to take advantage of the Firepower System's network-based advanced malware protection (AMP) capabilities.

See the following sections for more information:

Firepower 8000 Series Chassis Front View

The Firepower 8000 Series chassis can be in the AMP8x50, 81xx Family, the 82xx Family, or the 83xx Family. See the *Regulatory Compliance and Safety Information for FirePOWER and FireSIGHT Appliances* document for safety considerations for AMP8x50, 81xx Family, 82xx Family, and 83xx Family appliances.

AMP8x50 and Firepower 81xx Family Chassis Front View

The front view of the chassis contains the solid-state disk drive, LCD panel, front panel, and three module slots.

Figure 2-1   AMP8x50 and Firepower 81xx Family (Chassis: CHAS-1U-AC/DC) Front View
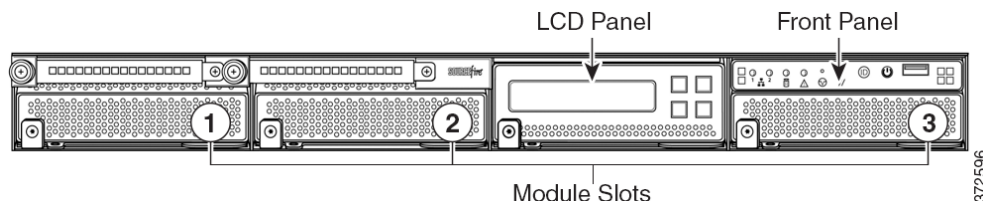
Firepower 82xx Family and Firepower and AMP 83xx Family Chassis Front View

The front view of the chassis contains the LCD panel, front panel, and seven module slots.

Figure 2-2   *Firepower 82xx Family (Chassis: CHAS-2U-AC/DC) and Firepower and AMP 83xx Family (PG35-2U-AC/DC) Front View*
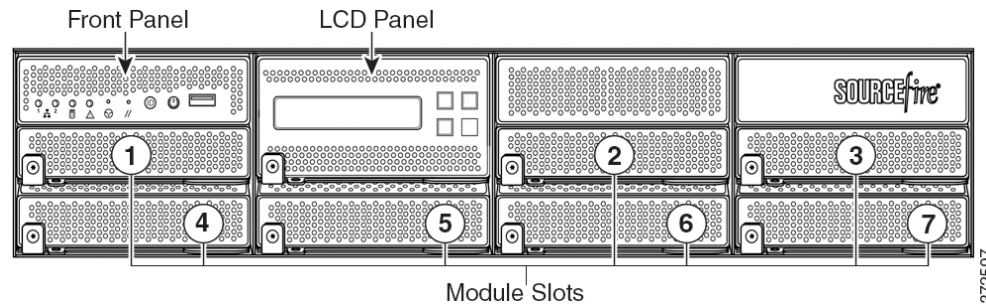
The following table describes the features on the front of the appliance.

Table 2-1   *Firepower 8000 Series System Components: Front View*

Feature	Description
Solid-state disk drive (81xx Family, AMP8x50)	Houses a solid-state drive (SSD) that functions as the primary system drive used for the operating system, the Firepower System software, and local file storage of events and configuration files.
	See Installing a Malware Storage Pack, page C-1 for information about installing an optional second SSD for expanded local file storage of suspected malware.
Module slots	Contain the modules. For information on available modules, see Firepower 8000 Series Modules, page 2-13.
LCD panel	Operates in multiple modes to configure the device, display error messages, and view system status. For more information, see Using the LCD Panel on a Firepower Device, page 4-1.
Front panel controls	Houses LEDs that display the system's operating state, as well as various controls, such as the power button. For more information, see Figure 2-4Firepower 82xx Family and Firepower and AMP 83xx Family Front Panel, page 2-4.
Front panel USB port	The USB 2.0 port allows you to attach a keyboard to the device.

See the following sections for more information:

- Firepower 8000 Series Front Panel, page 2-3
- Firepower 8000 Series Chassis Rear View, page 2-6

Firepower 8000 Series Front Panel

The front panel for the Firepower and AMP 81xx Family, 82xx Family, and 83xx Family contain the same components.

Figure 2-3   ***Firepower 81xx Family Front Panel***
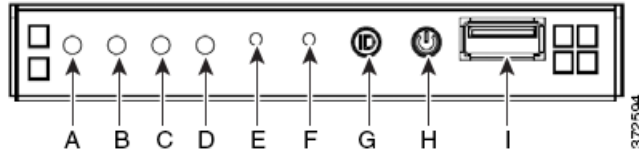
Figure 2-4   ***Firepower 82xx Family and Firepower and AMP 83xx Family Front Panel***
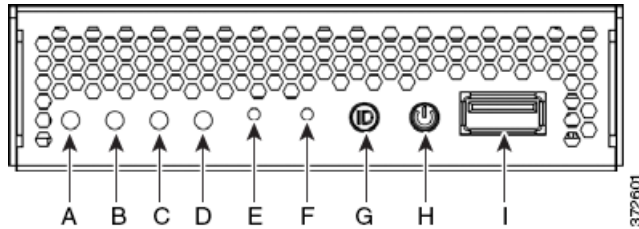
Table 2-2   ***Firepower 8000 Series Front Panel Components***

A	NIC activity LED	F	Reset button
B	Reserved	G	ID button
C	Solid-state drive activity LED	H	Power button and LED
D	System status LED	I	USB 2.0 connector
E	Non-maskable interrupt button		

The front panel of the chassis houses LEDs, which display the system's operating state. The following table describes the LEDs on the front panel

Table 2-3   ***Firepower 8000 Series Front Panel LEDs***

LED	Description
NIC activity	Indicates whether there is any network activity: • Green indicates there is network activity. • If the light is off, there is no network activity.
Solid-state drive activity	Indicates the SSD status: • Blinking green indicates the fixed disk drive is active. • Amber indicates a fixed disk drive fault. • If the light is off, there is no drive activity or the system is powered off.

Table 2-3   Firepower 8000 Series Front Panel LEDs (continued)

LED	Description
System status	Indicates the system status: • Green indicates the system is operating normally. • Blinking green indicates the system is operating in a degraded condition. • Blinking amber indicates the system is in a non-critical condition. • Amber indicates the system is in a critical or non-recoverable condition, or the system is starting up. • If the light is off, the system is starting up or off. **Note** The amber status light takes precedence over the green status light. When the amber light is on or blinking, the green light is off. See Table 2-4 on page 2-5 for more information.
System ID	Helps identify a system installed in a high-density rack with other similar systems: • A blue light indicates the ID button is pressed and a blue light is on at the rear of the appliance. • No light indicates the ID button is not pressed.
Power button and LED	Indicates whether the system has power: • Green indicates that the system has power. • If the light is off, the system does not have power.

The following table describes the conditions under which the system status LEDs might be lit.

Table 2-4   Firepower 8000 Series System Status

Condition	Description
Critical	Any critical or non-recoverable threshold crossing associated with the following events: • temperature, voltage, or fan critical threshold crossing • power subsystem failure • system inability to power up due to incorrectly installed processors or processor incompatibility • critical event logging errors, including System Memory Uncorrectable ECC error and fatal/uncorrectable bus errors, such as PCI SERR and PERR

Table 2-4   *Firepower 8000 Series System Status (continued)*

| Condition	Description
Non-critical	A non-critical condition is a threshold crossing associated with the following events: • temperature, voltage, or fan non-critical threshold crossing • chassis intrusion • Set Fault Indication command from system BIOS; the BIOS may use the command to indicate additional, non-critical status such as system memory or CPU configuration changes
Degraded	A degraded condition is associated with the following events: • one or more processors are disabled by Fault Resilient Boot (FRB) or BIOS • some system memory disabled or mapped out by BIOS • one of the power supplies unplugged or not functional **Tip** If you observe a degraded condition indication, check your power supply connections first. Power down the device, disconnect both power cords, reconnect the power cords to reseat them, and then restart the device. ⚠ **Caution** To power down safely, use the procedure in the Managing Devices chapter in the *Firepower Management Center Configuration Guide*, or the `system shutdown` command from the CLI.

Firepower 8000 Series Chassis Rear View

The Firepower 8000 Series chassis can be in the 81xx Family, 82xx Family, or 83xx Family.

AMP8x50 and Firepower 81xx Family Chassis Rear View

The rear of the chassis contains connection ports, the management interface, and the power supplies.

Figure 2-5   *AMP8x50 and Firepower 81xx Family (Chassis: CHAS-1U-AC/DC) Rear View*
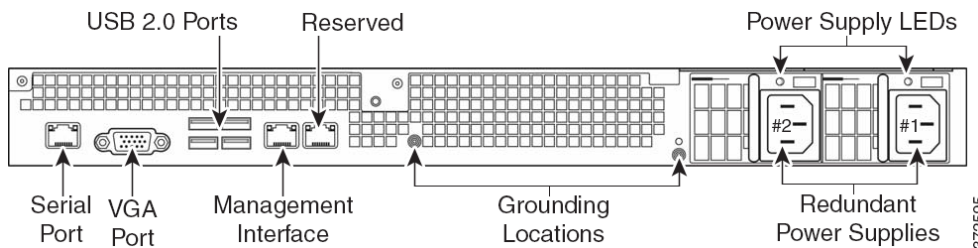
Firepower 82xx Family Chassis Rear View

The rear of the chassis contains power supplies, solid-state disk drives, connection ports, and the management interface.

Figure 2-6   Firepower 82xx Family (Chassis: CHAS-2U-AC/DC) Rear View
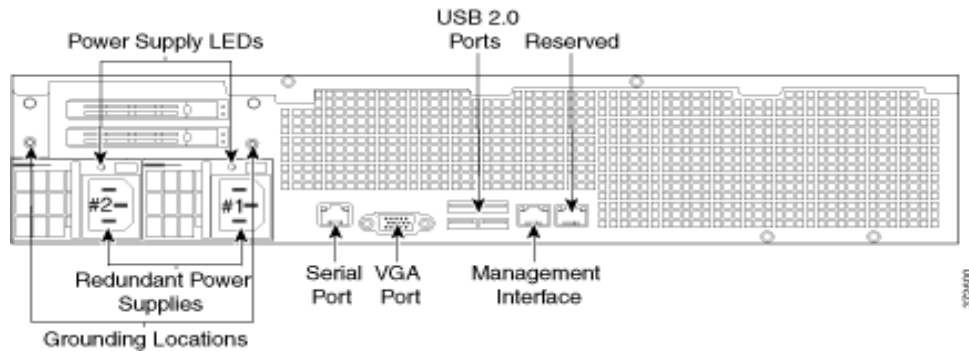
Firepower and AMP 83xx Family Chassis Rear View

The rear of the chassis contains power supplies, solid-state disk drives, connection ports, and the management interface.

Figure 2-7   Firepower and AMP 83xx Family (Chassis: PG35-2U-AC/DC) Rear View
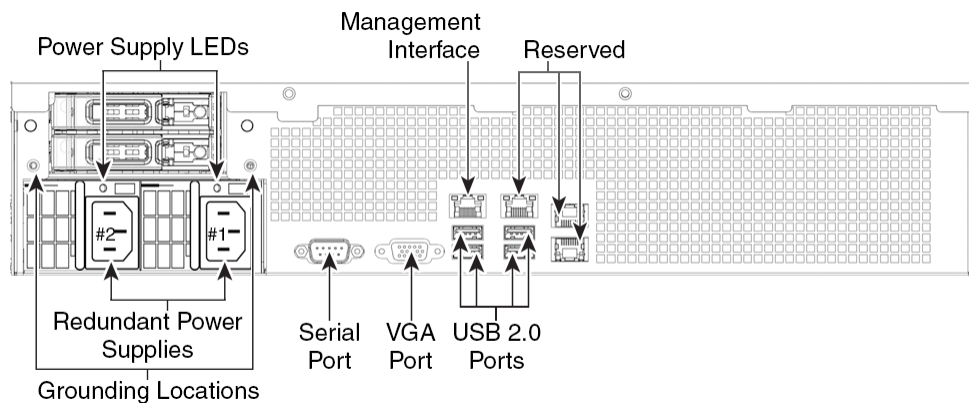
The following table describes the features that appear on the rear of the appliance.

Note   The Firepower 83xx Family hardware platform has six fans that display as FAN2 through FAN7. This is expected behavior. There is no FAN1 on the 83xx Family platform.

Table 2-5   Firepower 8000 Series System Components: Rear View

Feature	Description
VGA port USB 2.0 ports	Allows you to attach a monitor, keyboard, and mouse to the device, as an alternative to using the serial port, to establish a direct workstation-to-appliance connection.
RJ45 serial port (81xx Family and 82xx Family)	Allows you to establish a direct workstation-to-appliance connection (using an RJ45 to DB-9 adapter) for direct access to all of the management services on the device. The RJ45 serial port is used for maintenance and configuration purposes **only** and is not intended to carry service traffic.

Table 2-5   Firepower 8000 Series System Components: Rear View (continued)

Feature	Description
RS232 serial port (83xx Family)	Allows you to establish a direct workstation-to-appliance connection for direct access to all of the management services on the device. The RJ232 serial port is used for maintenance and configuration purposes **only** and is not intended to carry service traffic.
10/100/1000 Ethernet management interface	Provides for an out-of-band management network connection. The management interface is used for maintenance and configuration purposes **only** and is not intended to carry service traffic.
Redundant power supplies	Provides power to the device through an AC power source. Looking at the rear of the chassis, power supply #1 is on the right and power supply #2 is on the left.
Solid-state disk drive (82xx Family and 83xx Family)	Houses a solid-state drive (SSD) that functions as the primary system drive used for the operating system, the Firepower System software, and local file storage of events and configuration files.
Grounding locations	Allows you to connect the appliance to the Common Bonding Network. See the Power Requirements for Firepower 8000 Series Devices, page A-1 for more information.

The 10/100/1000 management interface is located on the rear of the appliance. The following table describes the LEDs associated with the management interface.

Table 2-6   Firepower 8000 Series Management Interface LEDs

LED	Description
Left (activity)	Indicates activity on the port: • A blinking light indicates activity. • No light indicates there is no activity.
Right (link)	Indicates whether the link is up: • A light indicates the link is up. • No light indicates there is no link.

The power supply modules are located on the rear of the appliance. The following table describes the LEDs associated with the management interface.

Table 2-7   Firepower 8000 Series Power Supply LEDs

LED	Description
Off	The power supply is not plugged in.
Amber	No power supplied to this module. or A power supply critical event such as module failure, a blown fuse, or a fan failure; the power supply shuts down.
Blinking amber	A power supply warning event, such as high temperature or a slow fan; the power supply continues to operate.

Table 2-7   Firepower 8000 Series Power Supply LEDs (continued)

LED	Description
Blinking green	AC input is present; volts on standby, the power supply is switched off.
Green	The power supply is plugged in and on.

The following table lists the signals on a typical DB-9 serial connector and the corresponding pins on the device's RJ45 serial connectors. You can use this table to construct an adapter for serial connections.

Table 2-8   Firepower 8000 Series RJ45 to DB-9 Adapter Pin-Out

DB-9 Pin	Signal	Description	RJ45 Pin
1	DCD/DSR	Data carrier detect/data set ready	7
2	RD	Receive data	6
3	TD	Transmit data	3
4	DTR	Data terminal ready	2
5	GND	Ground	4 & 5
6		No connection	
7	RTS	Request to send	1
8	CTS	Clear to send	8
9		No connection	

Firepower 8000 Series Physical and Environmental Parameters

The following table describes the physical attributes and environmental parameters for AMP8x50 and 81xx Family devices.

Table 2-9   AMP8x50 and 81xx Family Physical and Environmental Parameters

Parameter	Description
Form factor	1U
Dimensions (D x W x H)	28.7 in. x 17.2 in. x 1.73 in. (72.8 cm x 43.3 cm x 4.4 cm)
Weight maximum installed	43.5 lbs (19.8 kg)
Copper 1000BASE-T configurable bypass NetMod	Quad-port Gigabit copper Ethernet configurable bypass interfaces in a paired configuration Cable and distance: Cat5E at 50 m
Fiber 10GBASE configurable bypass MMSR or SMLR NetMod	Dual-port fiber configurable bypass interfaces with LC connectors Cable and distance: LR is single-mode at 5000 m (available) SR is multimode fiber (850 nm) at 550 m (standard)
Fiber 1000BASE-SX configurable bypass NetMod	Quad-port fiber configurable bypass interfaces 1000BASE-SX with LC connectors Cable and distance: SX is multimode fiber (850 nm) at 550 m (standard)

Table 2-9   *AMP8x50 and 81xx Family Physical and Environmental Parameters (continued)*

Parameter	Description
Copper 1000BASE-T non-bypass NetMod	Quad-port Gigabit copper Ethernet non-bypass interfaces in a paired configuration Cable and distance: Cat5E at 50 m

Fiber 10GBASE non-bypass MMSR or SMLR NetMod	Quad-port fiber non-bypass interfaces with LC connectors
	Cable and distance:
	    LR is single-mode at 5000 m (available)
	    SR is multimode fiber (850 nm) at 550 m (standard)

Fiber 1000BASE-SX non-bypass NetMod	Quad-port fiber non-bypass interfaces 1000BASE-SX with LC connectors Cable and distance: SX is multimode fiber (850 nm) at 550 m (standard)

Power supply	Dual 650 W redundant power supplies designed for AC or DC.
	
	AC Voltage: 100 VAC to 240 VAC nominal (85 VAC to 264 VAC maximum)
	AC Current: 5.2A maximum over the full range, per supply
	          2.6A maximum for 187 VAC to 264 VAC, per supply
	AC Frequency range: 47 Hz to 63 Hz
	
	DC Voltage: -48 VDC nominal referenced to RTN
	          -40 VDC to -72 VDC maximum
	DC Current: 11A maximum, per supply

Solid-state drive (SSD)	200GB 2.5-inch SSD. See Installing a Malware Storage Pack, page C-1 for information about installing an optional second SSD for expanded local file storage of suspected malware.
Operating temperature	50°F to 95°F (10°C to 35°C)
Non-operating temperature	-29°F to 158°F (-20°C to 70°C)
Operating humidity	5% to 85% non-condensing
Non-operating humidity	5% to 90%, non-condensing with a maximum wet bulb of 82^oF (28^oC) at temperatures from 77°F to 95°F (25°C to 35°C)
Altitude	0ft (sea level) to 6000 ft (0 to 1800 m)
Cooling requirements	1725 BTU/hour You must provide sufficient cooling to maintain the appliance within its required operating temperature range. Failure to do this may cause a malfunction or damage to the appliance.
Acoustic noise	Max normal operating noise is 87.6 dB LWAd (high temperature). Typical normal operating noise is 80 dB LWAd.
Operating shock	No errors with half a sine wave shock of 2G (with 11 ms duration)
Airflow	160 ft^3 (4.5 m^3) per minute Restriction of the airflow such as blocking the front or back or enclosing the unit in a cabinet without sufficient clearance may cause the unit to overheat, even if the ambient temperature is in the operating range. Airflow through the appliance enters at the front and exits at the rear. The minimum recommended clearance in the front and back is 7.9 in. (20 cm). This minimum can only be used if you can ensure a supply of low temperature air at the front of the appliance.

The following table describes the physical attributes and environmental parameters for Firepower 82xx Family and the Firepower and AMP 83xx Family devices.

Table 2-10   Firepower 82xx Family and Firepower and AMP 83xx Family Physical and Environmental Parameters

Parameter	Description	
Form factor	2U	
Dimensions (D x W x H)	29.0 in. x 17.2 in. x 3.48 in. (73.5 cm x 43.3 cm x 88.2 cm)	
Weight maximum installed	82xx Family:	58 lbs (25.3 kg)
	83xx Family:	67 lbs (30.5 kg)
Copper 1000BASE-T configurable bypass NetMod	Quad-port Gigabit copper Ethernet configurable bypass interfaces in a paired configuration Cable and distance: Cat5E at 50 m	

Fiber 10GBASE MMSR or SMLR configurable bypass NetMod	Dual-port fiber configurable bypass interfaces with LC connectors
	Cable and distance:
	    LR is single-mode at 5000 m (available)
	    SR is multimode fiber (850 nm) at 550 m (standard)	

Fiber 1000BASE-SX configurable bypass NetMod	Quad-port fiber configurable bypass interfaces1000BASE-SX with LC connectors Cable and distance: SX is multimode fiber (850 nm) at 550 m (standard)	

Fiber 40GBASE-SR4 configurable bypass NetMod	Dual-port fiber configurable bypass interfaces with OTP/MTP connectors
	Cable and distance:
	    OM3: 100 m at 850 nm Multimode
	    OM4: 150 m at 850 nm Multimode	

Copper 1000BASE-T non-bypass NetMod	Quad-port Gigabit copper Ethernet non-bypass interfaces in a paired configuration Cable and distance: Cat5E at 50 m	

Fiber 10GBASE non-bypass MMSR or SMLR NetMod	Quad-port fiber non-bypass interfaces with LC connectors
	Cable and distance:
	    LR is single-mode at 5000 m (available)
	    SR is multimode fiber (850 nm) at 550 m (standard)	

Fiber 1000BASE-SX non-bypass NetMod	Quad-port fiber non-bypass interfaces 1000BASE-SX with LC connectors Cable and distance: SX is multimode fiber (850 nm) at 550 m (standard)	

Table 2-10   Firepower 82xx Family and Firepower and AMP 83xx Family Physical and Environmental Parameters

Parameter	Description	
Power supply	82xx Family:	Dual 750 W redundant power supplies designed for AC or DC.
		AC Voltage: 100 VAC to 240 VAC nominal (85 VAC to 264 VAC maximum)
		AC Current: 8A maximum over the full range, per supply 4A maximum for 187 VAC to 264 VAC, per supply
		AC Frequency range: 47 Hz to 63 Hz
		DC Voltage: -48 VDC nominal referenced to RTN -40 VDC to -72 VDC maximum
		DC Current: 18A maximum, per supply
	83xx Family:	Dual 1000 W redundant power supplies designed for AC or DC.
		AC Voltage: 100 VAC to 240 VAC nominal (85 VAC to 264 VAC maximum)
		AC Current: 11A maximum over the full range, per supply 5.5A maximum for 187 VAC to 264 VAC, per supply
		AC Frequency range: 47 Hz to 63 Hz
		DC Voltage: -48 VDC nominal referenced to RTN -40 VDC to -72 VDC maximum
		DC Current: 25A maximum, per supply
Solid-state drive (SSD)	82xx Family:	200GB 2.5-inch SSD.
	83xx Family:	800GB 2.5-inch SSD.
	See Installing a Malware Storage Pack, page C-1 for information about installing an optional second SSD for expanded local file storage of suspected malware.	
Operating temperature	82xx Family:	50°F to 95°F (10°C to 35°C)
	83xx Family:	41°F to 104°F (5°C to 40°C)
Non-operating temperature	-29ºF to 158ºF (-20ºC to 70ºC)	
Operating humidity	5% to 85% non-condensing	
Non-operating humidity	5% to 90%, non-condensing with a maximum wet bulb of 82°F (28°C) at temperatures from 77°F to 95°F (25°C to 35°C)	
Altitude	0 ft (sea level) to 6000 ft (0 to 1800 m)	
Cooling requirements	up to 2900 BTU/hour You must provide sufficient cooling to maintain the appliance within its required operating temperature range. Failure to do this may cause a malfunction or damage to the appliance.	
Acoustic noise	Max normal operating noise is 81.6 dB LWAd (high temperature). Typical normal operating noise is 81.4 dB LWAd.	

Table 2-10   Firepower 82xx Family and Firepower and AMP 83xx Family Physical and Environmental Parameters

Parameter	Description
Operating shock	No errors with half a sine wave shock of 2G (with 11 ms duration)
Airflow	Front to back, 210 ft^3 (6 m^3) per minute
	Restriction of the airflow such as blocking the front or back or enclosing the unit in a cabinet without sufficient clearance may cause the unit to overheat, even if the ambient temperature is in the operating range.
	Airflow through the appliance enters at the front and exits at the rear. The minimum recommended clearance in the front and back is 7.9 in. (20cm). This minimum can only be used if you can ensure a supply of low temperature air at the front of the appliance.

Firepower 8000 Series Modules

The sensing interfaces for the Firepower 8000 Series appliances can be delivered with copper or fiber interfaces.

⚠

Caution   Modules are **not** hot-swappable. See Inserting and Removing Firepower 8000 Series Network Modules, page B-1 for more information.

The following modules contain configurable bypass sensing interfaces:

- a quad-port 1000BASE-T copper interface with configurable bypass capability. See Quad-Port 1000BASE-T Copper Configurable Bypass NetMod, page 2-13.

- a quad-port 1000BASE-SX fiber interface with configurable bypass capability. See Quad-Port 1000BASE-SX Fiber Configurable Bypass NetMod, page 2-14 for more information.

- a dual-port 10GBASE (MMSR or SMLR) fiber interface with configurable bypass capability. See Dual-Port 10GBASE (MMSR or SMLR) Fiber Configurable Bypass NetMod, page 2-16 for more information.

- a dual-port 40GBASE-SR4 fiber interface with configurable bypass capability (2U devices only). See Dual-Port 40GBASE-SR4 Fiber Configurable Bypass NetMod, page 2-17 for more information.

The following modules contain non-bypass sensing interfaces:

- a quad-port 1000BASE-T copper interface without bypass capability. See Quad-Port 1000BASE-T Copper Non-Bypass NetMod, page 2-19 for more information.

- a quad-port 1000BASE-SX fiber interface without bypass capability. See Quad-Port 1000BASE-SX Fiber Non-Bypass NetMod, page 2-19 for more information.

- a quad-port 10GBASE (MMSR or SMLR) fiber interface without bypass capability. See Quad-Port 10GBASE (MMSR or SMLR) Fiber Non-Bypass NetMod, page 2-20 for more information.

In addition, you can use a stacking module to connect two Firepower 8140, up to four Firepower 8250, or up to four Firepower or AMP 8350 devices to combine their processing power and increase throughput. See Stacking Module, page 2-21 for more information.

Quad-Port 1000BASE-T Copper Configurable Bypass NetMod

The quad-port 1000BASE-T copper configurable bypass NetMod contains four copper ports and link, activity, and bypass LEDs.

Activity LED

Link LED   Bypass LED
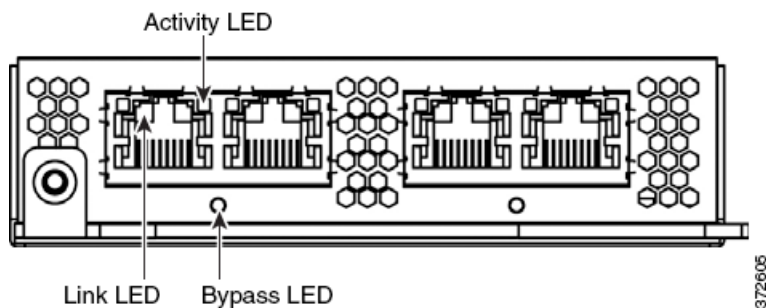
Use the following table to understand the link and activity LEDs on copper interfaces.

Table 2-11   *Copper Link/Activity LEDs*

Status	Description
Both LEDs off	The interface does not have link and is not in bypass mode.
Link amber	The speed of the traffic on the interface is 10Mb or 100Mb.
Link green	The speed of the traffic on the interface is 1Gb.
Activity blinking green	The interface has link and is passing traffic.

Use the following table to understand the bypass LEDs on copper interfaces.

Table 2-12   *Copper Bypass LEDs*

Status	Description
Off	The interface does not have link and is not in bypass mode.
Steady green	The interface has link and is passing traffic.
Steady amber	The interface has been intentionally brought down.
Blinking amber	The interface is in bypass mode; that is, it has failed open.

Quad-Port 1000BASE-SX Fiber Configurable Bypass NetMod

The quad-port 1000BASE-SX fiber configurable bypass NetMod contains four fiber ports and link, activity, and bypass LEDs.

Link LED   Ports

Activity LED   Bypass LED
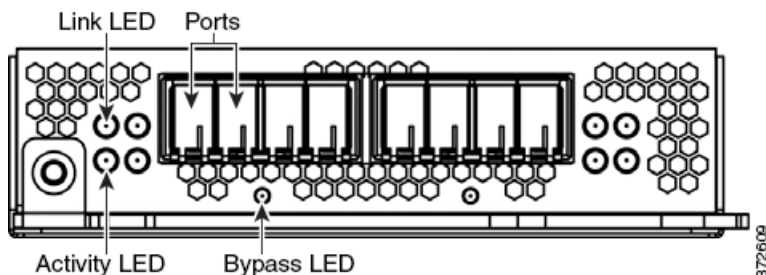
Use the following table to understand link and activity LEDs of the fiber interfaces.

Table 2-13   Fiber Link/Activity LEDs

Status	Description
Top	For an inline or passive interface: • A blinking light indicates the interface has activity. • No light indicates there is no activity.
Bottom	For an inline interface: • A light indicates the interface has activity. • No light indicates there is no activity. For a passive interface, the light is always on.

Use the following table to understand bypass LEDs on the fiber interfaces.

Table 2-14   Fiber Bypass LEDs

Status	Description
Off	The interface does not have link and is not in bypass mode.
Steady green	The interface has link and is passing traffic.
Steady amber	The interface has been intentionally brought down.
Blinking amber	The interface is in bypass mode; that is, it has failed open.

Use the following table to understand the optical specifications of the fiber interfaces.

Table 2-15   1000BASE-SX NetMod Optical Parameters

Parameter	1000BASE-SX
Optical connectors	LC duplex
Bit rate	1000Mbps
Baud rate/encoding/tolerance	1250Mbps 8b/10b encoding
Optical interface	Multimode
Operating distances	656 ft (200 m) for 62.5 μm/125 μm fiber 1640 ft (500 m) for 50 μm/125 μm fiber
Transmitter wavelength	770-860 nm (850 nm typical)
Maximum average launch power	0 dBm
Minimum average launch power	-9.5 dBm
Maximum average power at receiver	0 dBm
Receiver sensitivity	-17 dBm

Dual-Port 10GBASE (MMSR or SMLR) Fiber Configurable Bypass NetMod

The dual-port 10GBASE (MMSR or SMLR) fiber configurable bypass NetMod contains two fiber ports and link, activity, and bypass LEDs.

Use the following table to understand link and activity LEDs of the fiber interfaces.

Table 2-16   Fiber Link/Activity LEDs

Status	Description
Top	For an inline or passive interface: • A blinking light indicates the interface has activity. • No light indicates there is no activity.
Bottom	For an inline interface: • A light indicates the interface has activity. • No light indicates there is no activity. For a passive interface, the light is always on.

Use the following tables to understand the bypass LEDs on the fiber interfaces.

Table 2-17   Fiber Bypass LEDs

Status	Description
Off	The interface does not have link and is not in bypass mode.
Steady green	The interface has link and is passing traffic.
Steady amber	The interface has been intentionally brought down.
Blinking amber	The interface is in bypass mode; that is, it has failed open.

Use the following table to understand the optical parameters of the fiber interfaces.

Table 2-18   10GBASE MMSR and SMLR NetMod Optical Parameters

Parameter	10GBASE MMSR	10GBASE SMLR
Optical connectors	LC duplex	LC duplex
Bit rate	10.000Gbps	10.000Gbps
Baud rate/encoding/tolerance	10.3125Gbps 64/66b encoding +/- 100 ppm	10.3125Gbps 64/166b encoding +/- 100 ppm

Table 2-18   *10GBASE MMSR and SMLR NetMod Optical Parameters (continued)*

Parameter	10GBASE MMSR	10GBASE SMLR
Optical interface	Multimode	Single mode only
Operating distance	840-860 nm (850 nm typical)	1270-1355 nm (1310 nm typical)
	85 ft (26 m) to 108 ft (33 m) for 62.5 µm/125 µm fiber (modal BW 160 to 200 respectively)	6 ft to 6.2 miles (2 m to 10 km) for 9 µm/125 µm fiber
	216 ft (66 m) to 269 ft (82 m) for 50 µm/125 µm fiber (modal BW 400 to 500 respectively)	
	Distances to 980 ft (300 m) are available with higher quality (OM3) fiber.	
	Minimum distances (all): 6ft (2 m)	
Transmitter wavelength	840-860 nm (850 nm typical)	1270-1355 nm (1310 nm typical)
Maximum average launch power	-1 dBm	-0.5 dBm
Minimum average launch power	-7.3 dBm	-8.2 dBm
Maximum average power at receiver	-1 dBm	-0.5 dBm
Receiver sensitivity	-9.9 dBm	-14.4 dBm

Dual-Port 40GBASE-SR4 Fiber Configurable Bypass NetMod

The dual-port 40GBASE-SR4 fiber configurable bypass NetMod contains two fiber ports and link, activity, and bypass LEDs.
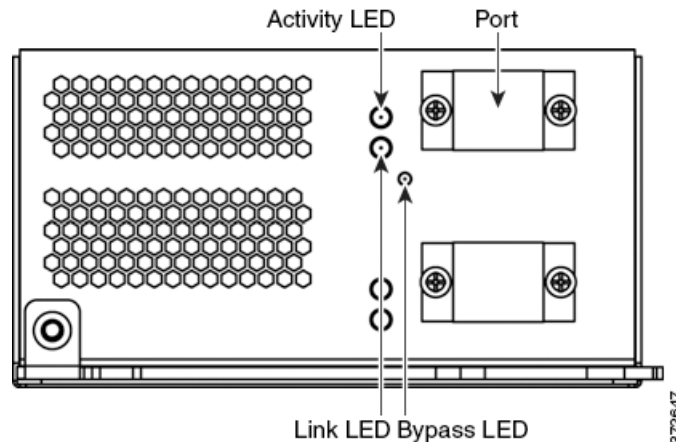
You can use the 40G NetMod in the following 8000 Series models:

- Firepower 8270 and 8290

- Firepower and AMP 8360, 8370 and 8390

- Firepower 8250 and 8260 (must be 40G-capable)

• Firepower and AMP 8350 (must be 40G-capable)

Caution   If you attempt to create a 40G interface on a device that is not 40G-capable, the 40G interface screen on its managing Firepower Management Center web interface displays red. A 40G-capable 8250 displays "8250-40G" on the LCD Panel and a 40G-capable 8350 displays "8350-40G" on the LCD Panel. See Firepower 8000 Series Modules, page 3-4 for placement information.

Use the following table to understand link and activity LEDs of the fiber interfaces.

Table 2-19   Fiber Link/Activity LEDs

Status	Description
Top (activity)	The light flashes when the interface has activity. If dark, there is no activity.
Bottom (link)	The light is on when the interface has link. If dark, there is no link.

Use the following table to understand bypass LED of the fiber interfaces.

Table 2-20   Fiber Bypass LED

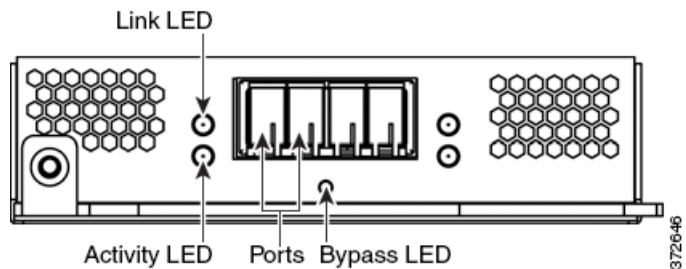| Status	Description
Off	The interface pair does not have link and is not in bypass mode, or has no power.
Steady green	The interface pair has link and is passing traffic.
Steady amber	The interface has been intentionally brought down.
Blinking amber	The interface is in bypass mode; that is, it has failed open.

Use the following table to understand optical parameters of the fiber interfaces.

Table 2-21   40GBASE-SR4 NetMod Optical Parameters

Parameter	40GBASE-SR4
Optical connectors	OTP/MTP single row twelve fiber positions. Only the outer eight fibers are used.
Bit rate	40.000Gbps
Baud rate/encoding/tolerance	10.3125Gbps 64/66b encoding +/- 100 ppm
Optical interface	Multimode
Operating distances	320 ft (100 m) for 50 μm/125 μm fiber (OM3) Minimum distance: 2 ft (0.5 m) 40G optics are carried on eight fiber cables utilizing MPO connectors.
Transmitter wavelength	840-860 nm (850 nm typical)
Maximum average launch power	2.4 dBm

Table 2-21   40GBASE-SR4 NetMod Optical Parameters (continued)

Parameter	40GBASE-SR4
Minimum average launch power	-7.8 dBm
Maximum average power at receiver	2.4 dBm
Receiver sensitivity	-9.5 dBm

Quad-Port 1000BASE-T Copper Non-Bypass NetMod

The quad-port 1000BASE-T copper non-bypass NetMod contains four copper ports, and link and activity LEDs.
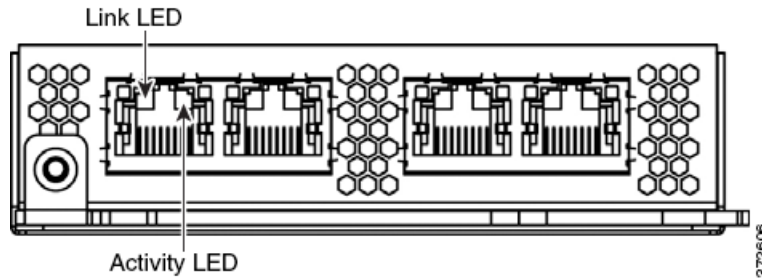
Use the following table to understand copper LEDs.

Table 2-22   Non-Bypass Copper Link/Activity LEDs

Status	Description
Both LEDs Off	The interface does not have link.
Link Amber	The speed of the traffic on the interface is 10Mb or 100Mb.
Link Green	The speed of the traffic on the interface is 1Gb.
Activity Blinking Green	The interface has link and is passing traffic.

Quad-Port 1000BASE-SX Fiber Non-Bypass NetMod

The quad-port 1000BASE-SX fiber non-bypass NetMod contains four fiber ports, and link and activity LEDs.
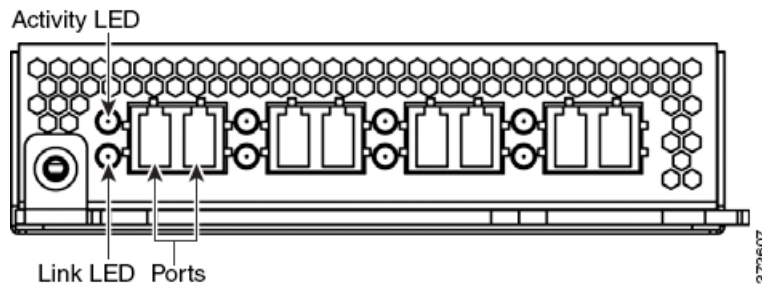
Use the following table to understand the link and activity LEDs on the fiber interfaces.

Table 2-23   Non-Bypass Fiber Link/Activity LEDs

Status	Description
Top (Activity)	For an inline or passive interface: the light flashes when the interface has activity. If dark, there is no activity.
Bottom (Link)	For an inline interface: the light is on when the interface has link. If dark, there is no link. For a passive interface: the light is always on.

Use the following table to understand the optical parameters of the fiber interfaces.

Table 2-24   1000BASE-SX NetMod Optical Parameters

Parameter	1000BASE-SX
Optical connectors	LC duplex
Bit rate	1000Mbps
Baud rate/encoding/tolerance	1250Mbps 8b/10b encoding
Optical interface	Multimode
Operating distances	656 ft (200 m) for 62.5 μm/125 μm fiber 1640 ft (500 m) for 50 μm/125 μm fiber
Transmitter wavelength	770-860 nm (850 nm typical)
Maximum average launch power	0 dBm
Minimum average launch power	-9.5 dBm
Maximum average power at receiver	0 dBm
Receiver sensitivity	-17 dBm

Quad-Port 10GBASE (MMSR or SMLR) Fiber Non-Bypass NetMod

The quad-port 10GBASE (MMSR or SMLR) fiber non-bypass NetMod contains four fiber ports, and link and activity LEDs.

⚠
Caution   The quad-port 10GBASE non-bypass NetMod contains non-removable SFPs. Any attempt to remove the SFP may damage the module.
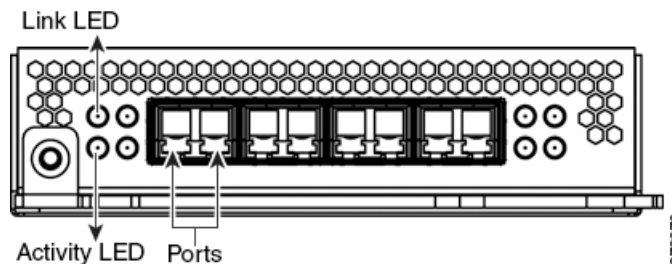
Use the following table to understand the link and activity LEDs on fiber interfaces.

Table 2-25   *Fiber Link/Activity LEDs*

Status	Description
Top	For an inline or passive interface: the light flashes when the interface has activity. If dark, there is no activity.
Bottom	For an inline interface: the light is on when the interface has link. If dark, there is no link.
	For a passive interface: the light is always on.

Use the following table to understand the optical parameters of the fiber interfaces.

*Table 2-26*   *10GBASE MMSR and SMLR NetMod Optical Parameters*

Parameter	10GBASE MMSR	10GBASE SMLR
Optical connectors	LC duplex	LC duplex
Bit rate	10.000Gbps	10.000Gbps
Baud rate/ encoding/tolerance	10.3125Gbps 64/66b encoding +/- 100 ppm	10.3125Gbps 64/66b encoding +/- 100 ppm
Optical interface	Multimode	Single mode only
Operating distance	840-860 nm (850 nm typical)	1270-1355 nm (1310 nm typical)
	85 ft (26 m) to 108 ft (33 m) for 62.5 μm/125 μm fiber (modal BW 160 to 200 respectively)	6 ft to 6.2 miles (2 m to 10 km) for 9 μm/125 μm fiber
	216 ft (66 m) to 269 ft (82 m) for 50 μm/125 μm fiber (modal BW 400 to 500 respectively)	
	Distances to 980 ft (300 m) are available with higher quality (OM3) fiber.	
	Minimum distances (all): 6ft (2 m)	
Transmitter wavelength	840-860 nm (850 nm typical)	1270-1355 nm (1310 nm typical)
Maximum average launch power	-1 dBm	-0.5 dBm
Minimum average launch power	-7.3 dBm	-8.2 dBm
Maximum average power at receiver	-1 dBm	-0.5 dBm
Receiver sensitivity	-9.9 dBm	-14.4 dBm

Stacking Module

The stacking module contains two connection ports for the 8000 Series stacking cable, and activity and link LEDs.
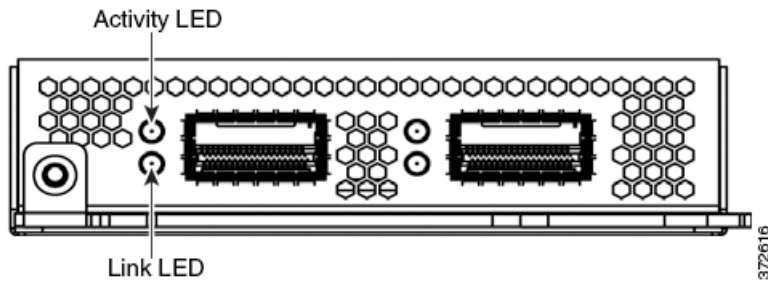
You can use the stacking module optionally in the following 8000 Series models:

- Firepower 8140 and 8250
- Firepower and AMP 8350

The stacking module is included in the following 8000 Series stacked configurations:

- Firepower 8260, 8270, and 8290
- Firepower and AMP 8360, 8370, and 8390

You can use the following table to understand the stacking LEDs.

Table 2-27   Stacking LEDs

Status	Description
Top	Indicates activity on the interface:
	• A blinking light indicates there is activity on the interface.
	• No light indicates there is no activity.
Bottom	Indicates whether the interface has link:
	• A light indicates the interface has link.
	• No light indicates there is no link.

Installing a Firepower 8000 Series Device

Firepower System appliances are easily installed on your network as part of a larger Firepower System deployment. You install devices on network segments to inspect traffic and generate intrusion events based on the intrusion policy applied to it. This data is transmitted to a Firepower Management Center, which manages one or more devices to correlate data across your full deployment, and coordinate and respond to threats to your security.

Tip You can use multiple management interfaces to improve performance or to isolate and manage traffic from two different networks. You configure the default management interface (eth0) during the initial installation. You can configure additional management interfaces after installation from the user interface. For more information, see *Firepower Management Center Configuration Guide*.

You can pre-configure multiple appliances at one location to be used in different deployment locations. For guidance on pre-configuring, see the *Firepower 8000 Series Getting Started Guide*.

Unpacking and Inspecting the Appliance

Tip Keep the shipping container in case the server requires shipping in the future.

Note The chassis is thoroughly inspected before shipment. If any damage occurred during transportation or any items are missing, contact your customer service representative immediately.

To inspect the shipment, follow these steps:

Step 1 Remove the chassis from its cardboard container and save all packaging material.

Step 2 Compare the shipment to the following list of components that ship with Firepower 8000 Series devices. As you unpack the system and the associated accessories, check that your package contents are complete as follows:

- one appliance
- power cord (two power cords are included with appliances that include redundant power supplies)
- Category 5e Ethernet straight-through cables: two for a Firepower device

  • one rack-mounting kit

Step 3 Check for damage and report any discrepancies or damage to your customer service representative. Have the following information ready:

  • Invoice number of shipper (see the packing slip)

  • Model and serial number of the damaged unit

  • Description of damage

  • Effect of damage on the installation

Security Considerations

Before you install your appliance, Cisco recommends that you consider the following:

  • Locate your appliance in a lockable rack within a secure location that prevents access by unauthorized personnel.

  • Allow only trained and qualified personnel to install, replace, administer, or service the appliance.

  • Always connect the management interface to a secure internal management network that is protected from unauthorized access.

  • Identify the specific workstation IP addresses that can be allowed to access appliances. Restrict access to the appliance to only those specific hosts using Access Lists within the appliance's system policy. For more information, see the *Firepower Management Center Configuration Guide*.

Identifying the Management Interfaces

You connect each appliance in your deployment to the network using the management interface. This allows the Firepower Management Center to communicate with and administer the devices it manages. Refer to the correct illustration for your appliance as you follow the installation procedure.

Firepower 8000 Series

The Firepower 8120, 8130, 8140, and AMP8150 are available as 1U appliances. The following illustration of the rear of the chassis indicates the location of the default management interface.

Management Interface
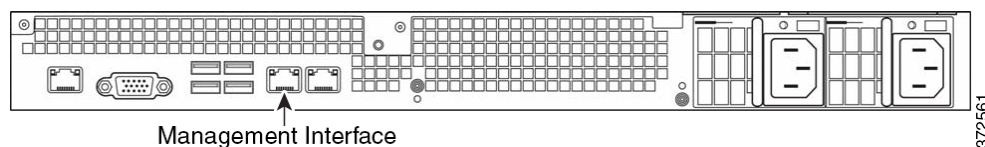
The Firepower 8250 is available as a 2U appliance. The Firepower 8260, 8270, and 8290 are available as 2U appliances with one, two, or three secondary 2U appliances. The following illustration of the rear of the chassis indicates the location of the default management interface for each 2U appliance.

Management Interface
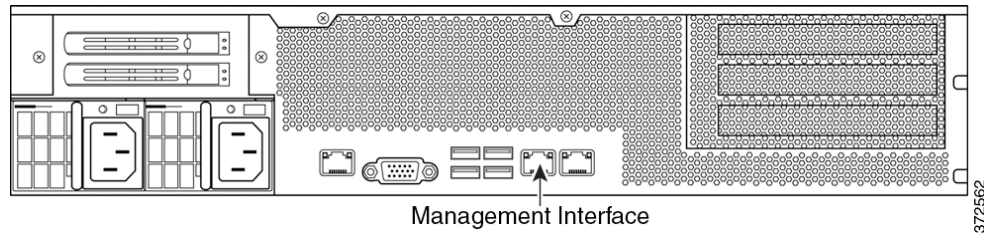
The Firepower and AMP 8350 is available as a 2U appliance. The Firepower and AMP 8360, 8370, and 8390 are available as 2U appliances with one, two, or three secondary 2U appliances. The following illustration of the rear of the chassis indicates the location of the default management interface for each 2U appliance.

Management Interface
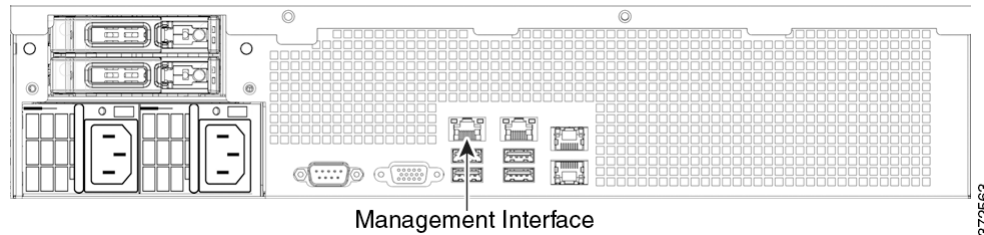
Identifying the Sensing Interfaces

Firepower devices connect to network segments using sensing interfaces. The number of segments each device can monitor depends on the number of sensing interfaces on the device and the type of connection (passive, inline, routed, or switched) that you want to use on the network segment.

The following sections describe the sensing interfaces for each Firepower device:

- To locate the sensing interfaces on the 8000 Series, see Firepower 8000 Series, page 3-3.

- To locate the module slots on the 8000 Series on the Firepower 8000 Series, page 3-3.

- To locate the sensing interfaces on the 8000 Series NetMods, see Firepower 8000 Series Modules, page 3-4.

For information on connection types, see Understanding Sensing Interfaces, page 6-2.

Firepower 8000 Series

The 8000 Series is available as a 1U device with a 10G network switch or a 2U device with either a 10G or a 40G network switch. This device can be shipped fully assembled, or you can install the network modules (NetMods) that contain the sensing interfaces.

Note   If you install a NetMod in an incompatible slot on your device (for example, inserting a 40G NetMod in slots 1 and 4 on a Firepower 8250 or Firepower or AMP 8350) or a NetMod is otherwise incompatible with your system, an error or warning message appears in the web interface of the managing Firepower Management Center when you attempt to configure the NetMod. Contact Support for assistance.

The following modules contain configurable bypass sensing interfaces:

- a quad-port 1000BASE-T copper interface with configurable bypass capability

- a quad-port 1000BASE-SX fiber interface with configurable bypass capability
- a dual-port 10GBASE (MMSR or SMLR) fiber interface with configurable bypass capability
- a dual-port 40GBASE-SR4 fiber interface with configurable bypass capability (2U devices only)

The following modules contain non-bypass sensing interfaces:

- a quad-port 1000BASE-T copper interface without bypass capability
- a quad-port 1000BASE-SX fiber interface without bypass capability
- a dual-port 10GBASE (MMSR or SMLR) fiber interface without bypass capability

In addition, a stacking module combines the resources of two or more identically configured appliances. The stacking module is optional on the Firepower 8140, 8250, and 8350; and is provided in the Firepower 8260, 8270, 8290 and the Firepower and AMP 8360, 8370, 8390 stacked configurations.

⚠️
Caution   Modules are **not** hot-swappable. See Inserting and Removing Firepower 8000 Series Modules, page B-1 for more information.

The following illustrations of the front of the chassis indicates the location of the module slots that contain the sensing interfaces.

Figure 3-1   *Firepower 81xx Family Front Chassis View*
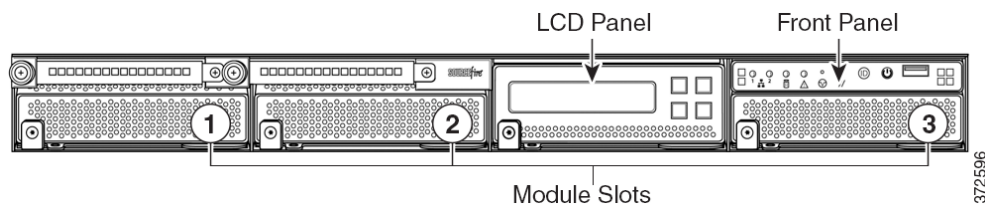
Figure 3-2   *Firepower 82xx Family and Firepower and AMP 83xx Family Front Chassis View*
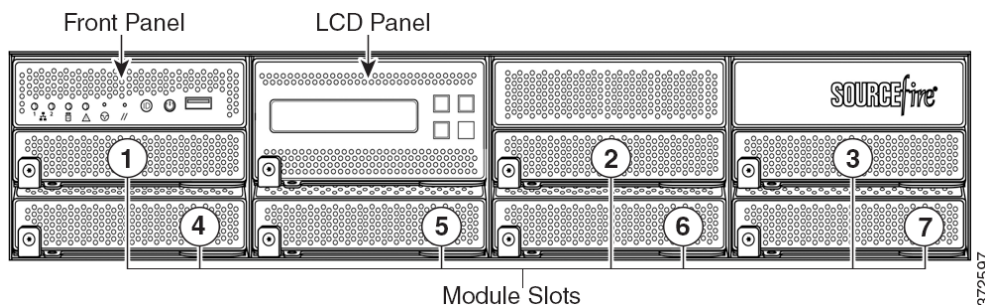
Firepower 8000 Series Modules

The Firepower 8000 Series can be delivered with the following modules with configurable bypass capability:

- a quad-port 1000BASE-T copper interface with configurable bypass capability. See Figure 3-3Quad-Port 1000BASE-T Copper Configurable Bypass NetMod, page 3-5 for more information.

- a quad-port 1000BASE-SX fiber interface with configurable bypass capability. See Figure 3-4Quad-Port 1000BASE-SX Fiber Configurable Bypass NetMod, page 3-6 for more information.

- a dual-port 10GBASE (MMSR or SMLR) fiber interface with configurable bypass capability. See Figure 3-5Dual-Port 10GBASE (MMSR or SMLR) Fiber Configurable Bypass NetMod, page 3-6 for more information.

- a dual-port 40GBASE-SR4 fiber interface with configurable bypass capability. See Figure 3-6Dual-Port 40GBASE-SR4 Fiber Configurable Bypass NetMod, page 3-7 for more information.

The Firepower 8000 Series can be delivered with the following modules without configurable bypass capability:

- a quad-port 1000BASE-T copper interface without bypass capability. See Figure 3-8Quad-Port 1000BASE-T Copper Non-Bypass NetMod, page 3-8 for more information.

- a quad-port 1000BASE-SX fiber interface without bypass capability. See Figure 3-9Quad-Port 1000BASE-SX Fiber Non-Bypass NetMod, page 3-8 for more information.

- a quad-port 10GBASE (MMSR or SMLR) fiber interface without bypass capability. See Figure 3-10Quad-Port 10GBASE (MMSR or SMLR) Fiber Non-Bypass NetMod, page 3-8 for more information.

A stacking module is optional on the Firepower 8140, 8250, and 8350; and is provided in the Firepower 8260, 8270, 8290 and the Firepower 8360, 8370, 8390 stacked configurations. See Firepower 8000 Series Stacking Module, page 3-9 for more information.

Figure 3-3   Quad-Port 1000BASE-T Copper Configurable Bypass NetMod
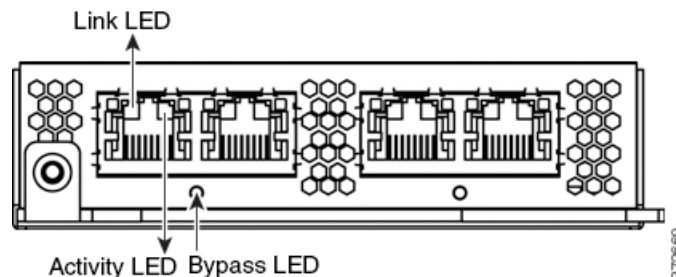
You can use these connections to passively monitor up to four separate network segments. You also can use paired interfaces in inline or inline with bypass mode, which allows you to deploy the device as an intrusion prevention system on up to two networks.

If you want to take advantage of the device's automatic bypass capability, you must connect either the two interfaces on the left or the two interfaces on the right to a network segment. This allows traffic to flow even if the device fails or loses power. You must also use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

Figure 3-4   Quad-Port 1000BASE-SX Fiber Configurable Bypass NetMod
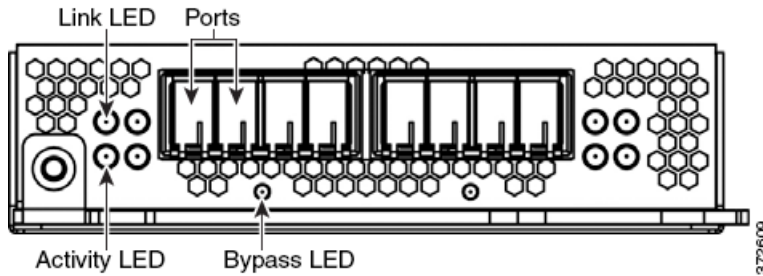
The quad-port 1000BASE-SX fiber configurable bypass configuration uses LC-type (Local Connector) optical transceivers.

You can use this configuration to passively monitor up to four separate network segments. You also can use paired interfaces in inline or inline with bypass mode, which allows you to deploy the managed device as an intrusion prevention system on up to two separate networks.

Tip   For best performance, use the interface sets consecutively. If you skip interfaces, you may experience degraded performance.

If you want to take advantage of a device's automatic bypass capability, you must connect the two interfaces on the left or the two interfaces on the right to a network segment. This allows traffic to flow even if the device fails or loses power. You must also use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

Figure 3-5   Dual-Port 10GBASE (MMSR or SMLR) Fiber Configurable Bypass NetMod
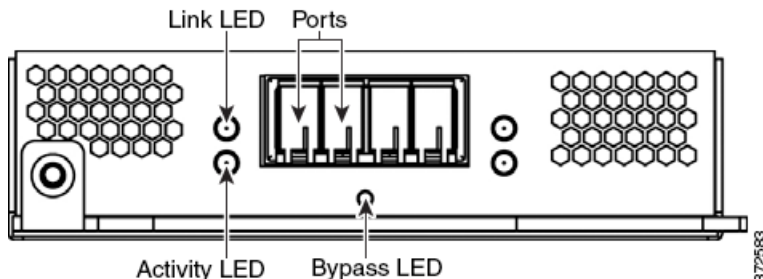
The dual-port 10GBASE fiber configurable bypass configuration uses LC-type (Local Connector) optical transceivers. Note that these can be either MMSR or SMLR interfaces.

You can use this configuration to passively monitor up to two separate network segments. You also can use paired interfaces in inline or inline with bypass mode, which allows you to deploy the managed device as an intrusion prevention system on a single network.

Tip   For best performance, use the interface sets consecutively. If you skip interfaces, you may experience degraded performance.

If you want to take advantage of a device's automatic bypass capability, you must connect two interfaces to a network segment. This allows traffic to flow even if the device fails or loses power. You must also use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

Figure 3-6   *Dual-Port 40GBASE-SR4 Fiber Configurable Bypass NetMod*
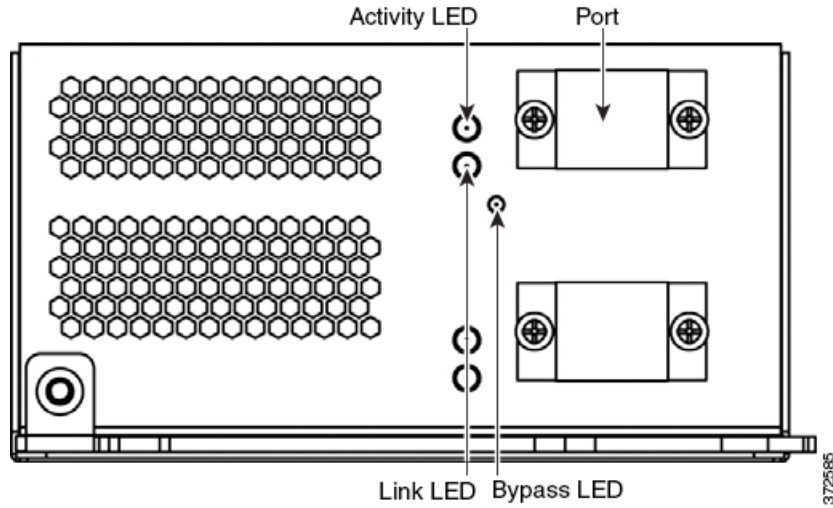
The dual-port 40GBASE-SR4 fiber configurable bypass configuration uses MPO (Multiple-Fiber Push On) connector optical transceivers.

You can use the 40G NetMod only in the following 8000 Series models:

- Firepower 8270 and 8290

- Firepower and AMP 8360, 8370 and 8390

- Firepower 8250 and 8260 (must be 40G-capable)

- Firepower and AMP 8350 (must be 40G-capable)

⚠️

Caution   If you attempt to create a 40G interface on a device that is not 40G-capable, the 40G interface screen on its managing Firepower Management Center web interface displays red. A 40G-capable 8250 displays "8250-40G" on the LCD Panel and a 40G-capable 8350 displays "8350-40G" on the LCD Panel.

You can use this configuration to passively monitor up to two separate network segments. You also can use the paired interface in inline or inline with bypass mode, which allows you to deploy the device as an intrusion prevention system on one network.

You can use up to two 40G NetMods. Install the first 40G NetMod in slots 3 and 7, and the second in slots 2 and 6. You cannot use a 40G NetMod in slots 1 and 4.

Figure 3-7   *40G NetMod Placement*

Not Available for 40G NetMod   Second 40G NetMod   First 40G NetMod
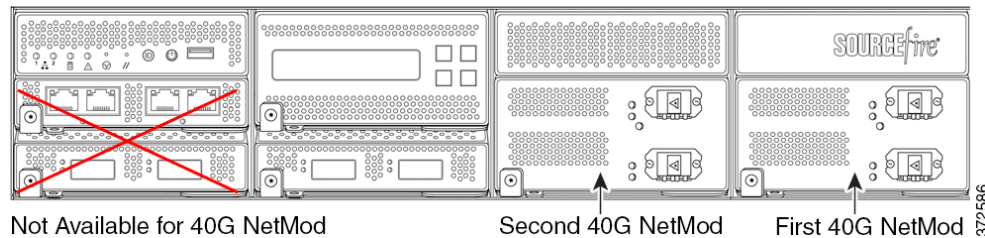
If you want to take advantage of a device's automatic bypass capability, you must use the web interface to configure a pair of interfaces as an inline set and enable bypass mode on the inline set.

Figure 3-8   Quad-Port 1000BASE-T Copper Non-Bypass NetMod
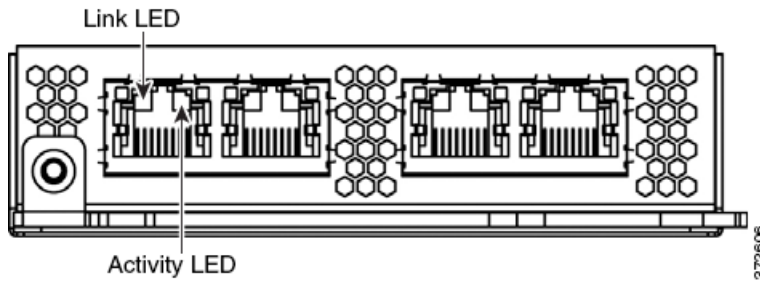
You can use these connections to passively monitor up to four separate network segments. You also can use paired interfaces in inline configuration on up to two network segments.

Figure 3-9   Quad-Port 1000BASE-SX Fiber Non-Bypass NetMod
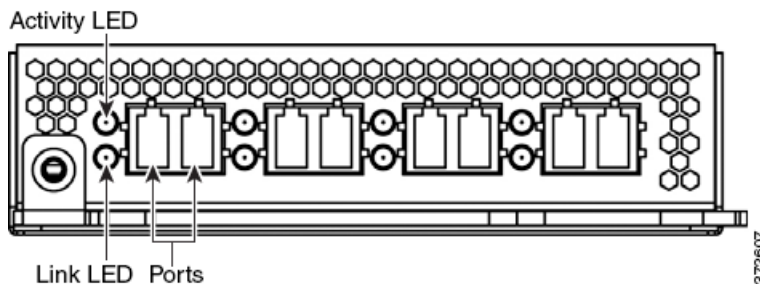
The quad-port 1000BASE-SX fiber non-bypass configuration uses LC-type (Local Connector) optical transceivers.

You can use these connections to passively monitor up to four separate network segments. You also can use paired interfaces in inline configuration on up to two network segments.

Tip   For best performance, use the interface sets consecutively. If you skip interfaces, you may experience degraded performance.

Figure 3-10   Quad-Port 10GBASE (MMSR or SMLR) Fiber Non-Bypass NetMod
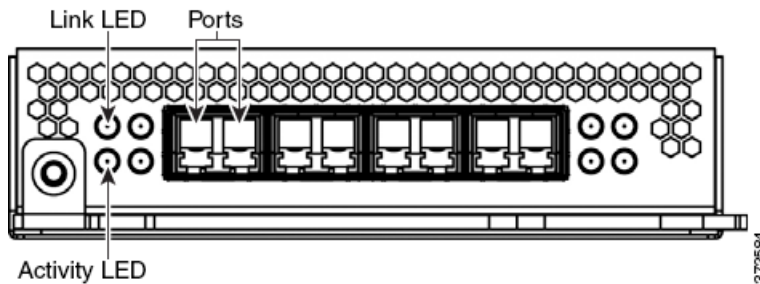
The quad-port 10GBASE fiber non-bypass configuration uses LC-type (Local Connector) optical transceivers with either MMSR or SMLR interfaces.

Caution   The quad-port 10G BASE non-bypass NetMod contains non-removable small form-factor pluggable (SFP) transceivers. Any attempt to remove the SFPs can damage the module.

You can use these connections to passively monitor up to four separate network segments. You also can use paired interfaces in inline configuration on up to two network segments.

Firepower 8000 Series Stacking Module

A stacking module combines the resources of two or more identically configured appliances. The stacking module is optional on the following 8000 Series models:

- Firepower 8140 and 8250
- Firepower and AMP 8350

The stacking module is included in the following 8000 Series stacked configurations:

- Firepower 8260, 8270, and 8290
- Firepower and AMP 8360, 8370, and 8390
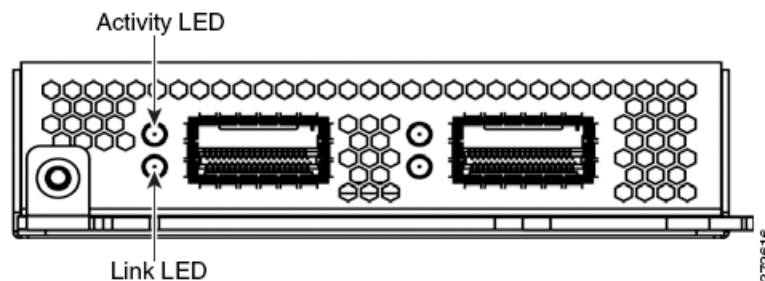
The stacking module allows you to combine the resources of two devices, using one as the primary device and one as the secondary. Only the primary device has sensing interfaces. The following devices can use the stacking module:

- The Firepower 8140, 8250, and 8350 can be delivered with the stacking module.
- The Firepower 8260 stacked configuration is delivered with one stacking module in the primary device and one stacking module in the secondary device.
- The Firepower and AMP 8360 stacked configurations are delivered with one stacking module in the primary device and one stacking module in the secondary device.
- The Firepower 8270 stacked configuration is delivered with two stacking modules in the primary device and one stacking module in each of the two secondary devices.
- The Firepower and AMP 8370 stacked configurations are delivered with two stacking modules in the primary device and one stacking module in each of the two secondary devices.
- The Firepower 8290 stacked configuration is delivered with three stacking modules in the primary device, and one stacking module in each of the three secondary devices.
- The Firepower and AMP 8390 stacked configurations are delivered with three stacking modules in the primary device, and one stacking module in each of the three secondary devices.

For more information on using stacked devices, see Using Devices in a Stacked Configuration.

Using Devices in a Stacked Configuration

You can increase the amount of traffic inspected on network segments by combining the resources of identically configured devices in a stacked configuration. One device is designated as the primary device and is connected to the network segments. All other devices are designated secondary devices, and are used to provide additional resources to the primary device. A Firepower Management Center creates, edits, and manages the stacked configuration.

The primary device contains sensing interfaces and one set of stacking interfaces for each secondary device connected to it. You connect the sensing interfaces on the primary device to the network segments you want to monitor in the same way as a non-stacked device. You connect the stacking interfaces on the primary device to the stacking interfaces on the secondary devices using the stacking cables. Each secondary device is connected directly to the primary device using the stacking interfaces. If a secondary device contains sensing interfaces, they are not used.

You can stack devices in the following configurations:

- two Firepower 8140s
- up to four Firepower 8250s
- a Firepower 8260 (a 10G-capable primary device and a secondary device)
- a Firepower 8270 (a 40G-capable primary device and two secondary devices)
- a Firepower 8290 (a 40G-capable primary device and three secondary devices)
- up to four Firepower or AMP 8350s
- a Firepower or AMP 8360 (a 40G-capable primary device and a secondary device)
- a Firepower or AMP 8370 (a 40G-capable primary device and two secondary devices)
- a Firepower or AMP 8390 (a 40G-capable primary device and three secondary devices)

For the Firepower 8260 and 8270 devices and Firepower or AMP 8360 and 8370 devices, you can stack additional devices for a total of four devices in the stack.

One device is designated as the primary device and is displayed on the Firepower Management Center's web interface with the primary role. All other devices in the stacked configuration are secondary and displayed in the web interface with the secondary role. You use the combined resources as a single entity except when viewing information from the stacked devices.

Connect the primary device to the network segments you want to analyze in the same way that you would connect a single Firepower 8140, Firepower 8250, and Firepower or AMP 8350. Connect the secondary devices to the primary device as indicated in the stack cabling diagram.

⚠
Caution   You **must** have management interfaces configured and working for all device stack members. Register all devices as single devices, stack them, and never remove or disable the management interfaces for stacked secondary devices. This allows each stack member to report health and exchange configuration information.

After the devices are physically connected to the network segments and to each other, use a Firepower Management Center to establish and manage the stack.

The following sections provide more information on how to connect and manage stacked devices:

- Connecting the Firepower 8140, page 3-11
- Connecting the Firepower 82xx Family and Firepower and AMP 83xx Family, page 3-11
- Using the 8000 Series Stacking Cable, page 3-14

- Managing Stacked Devices, page 3-15

Connecting the Firepower 8140

You can connect two Firepower 8140s in a stacked configuration. You must use one 8000 Series stacking cable to create the physical connection between the primary device and the secondary device. For more information on using the stacking cable, see Using the 8000 Series Stacking Cable, page 3-14.

Install the devices in your rack so you can easily connect the cable between the stacking modules. You can install the secondary device above or below the primary device.

Connect the primary device to the network segments you want to analyze in the same way that you would connect a single Firepower 8140. Connect the secondary device directly to the primary device.

The following graphic shows a primary device with a secondary device installed below the primary device.
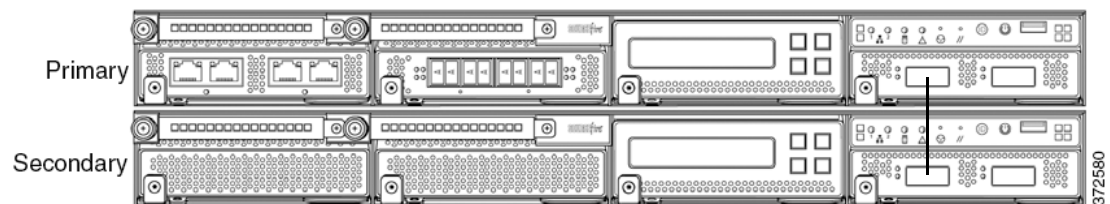
To connect a Firepower 8140 secondary device:

Step 1   Use an 8000 Series stacking cable to connect the left stacking interface on the primary device to the left stacking interface on the secondary device, then use the Firepower Management Center that manages the devices to establish the stacked device relationship in the system. Note that the right stacking interface is not connected. See Managing Stacked Devices, page 3-15.

⚠

Caution   You **must** have management interfaces configured and working for all device stack members. Register all devices as single devices, stack them, and never remove or disable the management interfaces for stacked secondary devices. This allows each stack member to report health and exchange configuration information.

Connecting the Firepower 82xx Family and Firepower and AMP 83xx Family

You can connect any of the following configurations:

- up to four 8250s
- up to four Firepower 8350s or four AMP8350s
- a Firepower 8260 (a 10G-capable primary device and a secondary device)
- a Firepower or AMP 8360 (a 40G-capable primary device and a secondary device)
- a Firepower 8270 (a 40G-capable primary device and two secondary devices)
- a Firepower or AMP 8370 (a 40G-capable primary device and two secondary devices)
- a Firepower 8290 (a 40G-capable primary device and three secondary devices)
- a Firepower or AMP 8390 (a 40G-capable primary device and three secondary devices)

You can stack additional devices for a total of four devices in the stack for the following configurations:

- Firepower 8260 and 8270
- Firepower or AMP 8360
- Firepower or AMP 8370

You must use two 8000 Series stacking cables for each secondary device you want to connect to the primary device. For more information on using the stacking cable, see Using the 8000 Series Stacking Cable, page 3-14.

Install the devices in your rack so you can easily connect the cables between the stacking modules. You can install the secondary devices above or below the primary device.

Connect the primary device to the network segments you want to analyze in the same way that you would connect a single Firepower 8250 or 8350 (Firepower or AMP). Connect each secondary device directly to the primary device as required for the number of secondary devices in the configuration.

⚠

Caution   You **must** have management interfaces configured and working for all device stack members. Register all devices as single devices, stack them, and never remove or disable the management interfaces for stacked secondary devices. This allows each stack member to report health and exchange configuration information.

8250 or 8350 Primary Device with One Secondary Device

The following example shows a Firepower 8250 or 8350 (Firepower or AMP) primary device and one secondary device. The secondary device is installed below the primary device. Note that the secondary device contains no sensing interfaces.
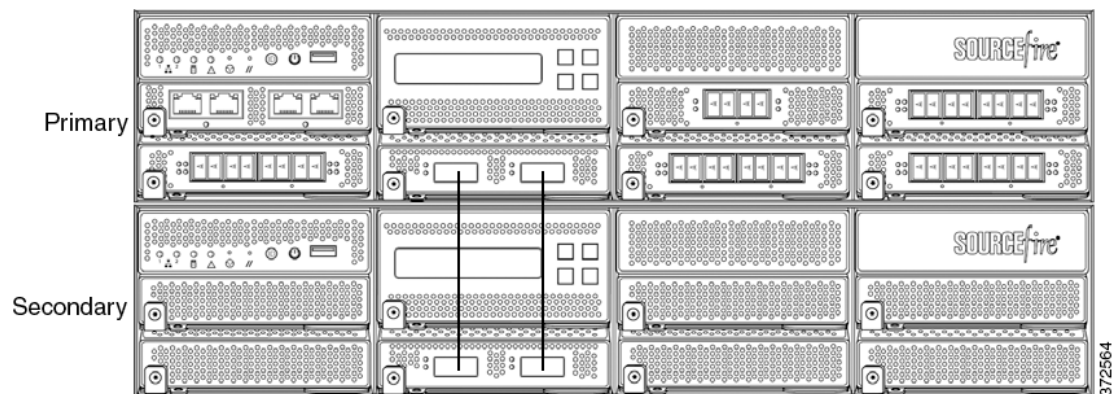
8260 or 8360 Primary Device and One Secondary Device

The following example shows a Firepower 8260 or a 8360 (Firepower or AMP) configuration. The Firepower 8260 includes a 10G-capable 8250 primary device and one dedicated secondary device. The Firepower or AMP 8360 includes a 40G-capable 8350 primary device and one dedicated secondary device. For each configuration (8260 or 8360), the secondary device is installed below the primary device.
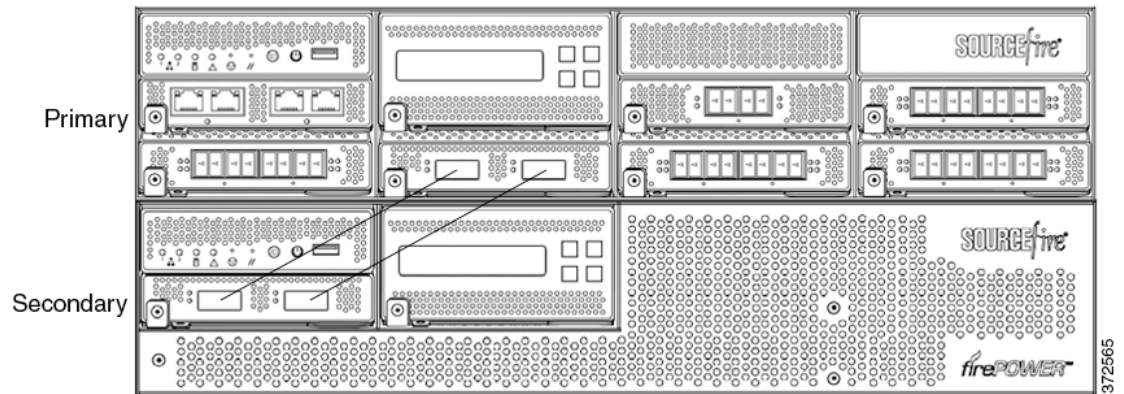
8270 or 8370 Primary Device (40G) and Two Secondary Devices

The following example shows a Firepower 8270 or a 8370 (Firepower or AMP) configuration. The Firepower 8270 includes a 40G-capable 8250 primary device and two dedicated secondary devices. The Firepower or AMP 8370 includes a 40G-capable 8350 primary device and two dedicated secondary devices. For each configuration (8270 or 8370), one secondary device is installed above the primary device and the other is installed below the primary device.
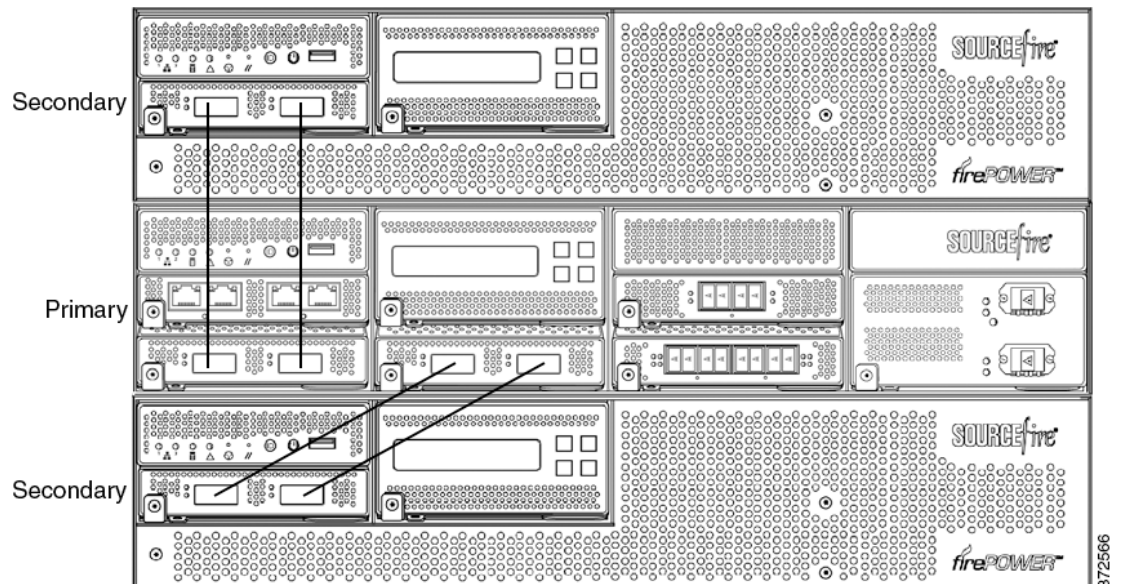
8290 or 8390 Primary Device (40G) and Three Secondary Devices

The following example shows a Firepower 8290 or a 8390 (Firepower or AMP) configuration. The Firepower 8290 includes a 40G-capable 8250 primary device and three dedicated secondary devices. The Firepower or AMP 8370 includes a 40G-capable 8350 primary device and two dedicated secondary devices. For each configuration (8290 or 8390), one secondary device is installed above the primary device and two secondary devices are installed below the primary device.
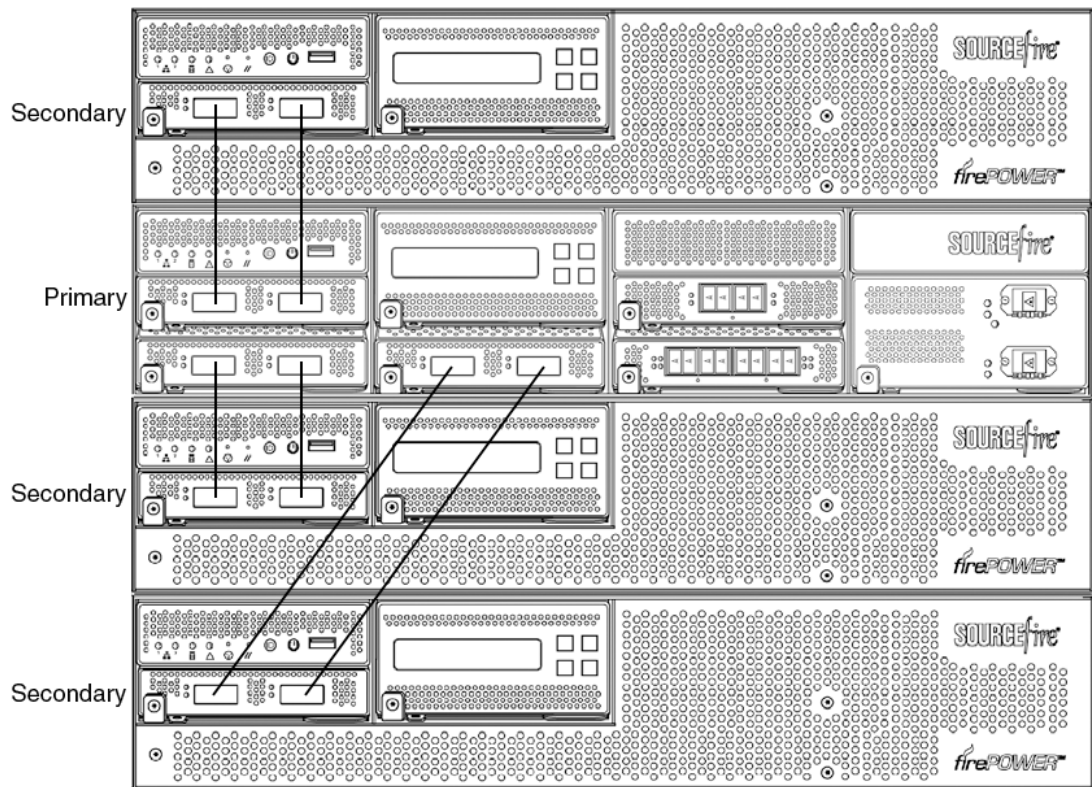
To connect a 8250 or a 8350 secondary device:

Step 1   Use an 8000 Series stacking cable to connect the left interface on the stacking module on the primary device to the left interface on the stacking module on the secondary device.

Step 2   Use a second 8000 Series stacking cable to connect the right interface on the stacking module on the primary device to the right interface on the stacking module on the secondary device.

Step 3   Repeat steps 1 and 2 for each secondary device you want to connect.

Step 4   Use the Firepower Management Center that manages the devices to establish the stacked device relationship and manage their joint resources. See Managing Stacked Devices, page 3-15.

⚠

Caution   You **must** have management interfaces configured and working for all device stack members. Register all devices as single devices, stack them, and never remove or disable the management interfaces for stacked secondary devices. This allows each stack member to report health and exchange configuration information.

Using the 8000 Series Stacking Cable

The 8000 Series stacking cable has identically-keyed ends, each with a latch to secure the cable in the device and a latch release tab.
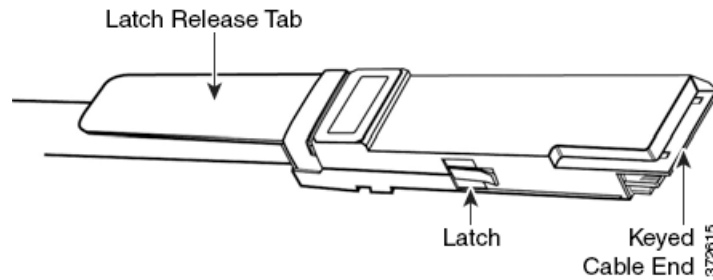
Use 8000 Series stacking cables to create the physical connection between the primary device and each secondary device as required for each device configuration:

- the Firepower 8250, 8260, 8270, and 8290 require two cables per connection
- the Firepower or AMP 8350, 8360, 8370, and 8390 require two cables per connection
- the Firepower 8140 requires one cable

Devices do not need to be powered down to insert or remove the stacking cable.

⚠

Caution   Use only the Cisco 8000 Series stacking cable when cabling your devices. Using unsupported cables can create unforeseen errors.

Use the Firepower Management Center to manage the stacked devices after you have physically connected the devices.

To insert an 8000 Series stacking cable:

Step 1   To insert the cable, hold the cable end with release tab facing up, then insert the keyed end into the port on the stacking module until you hear the latch click into place.

To remove an 8000 Series stacking cable:

Step 1   To remove the cable, pull on the release tab to release the latch, then remove the cable end.

Managing Stacked Devices

A Firepower Management Center establishes the stacked relationship between the devices, controls the interface sets of the primary device, and manages the combined resources in the stack. You cannot manage interface sets on the local web interface of a stacked device.

After the stacked relationship is established, each device inspects traffic separately using a single, shared detection configuration. If the primary device fails, traffic is handled according to the configuration of the primary device (that is, as if the stacked relationship did not exist). If the secondary device fails, the primary device continues to sense traffic, generate alerts, and send traffic to the failed secondary device where the traffic is dropped.

For information on establishing and managing stacked devices, see Managing Stacked Devices in the *Firepower Management Center Configuration Guide*.

Installing the Firepower Device in a Rack

You can rack-mount all Firepower devices. When you install an appliance, you must also make sure that you can access its console. To access the console for initial setup, connect to the appliance in one of the following ways:

Keyboard and Monitor/KVM

You can connect a USB keyboard and VGA monitor to a Firepower device, which is useful for rack-mounted appliances connected to a keyboard, video, and mouse (KVM) switch.

⚠

Caution   Do **not** use a KVM console with USB mass storage to access the appliance for the initial setup because the appliance may attempt to use the mass storage device as a boot device.

Ethernet Connection to Management Interface

Configure a local computer, which must not be connected to the Internet, with the following network settings:

- IP address: `192.168.45.2`

- netmask: `255.255.255.0`

- default gateway: `192.168.45.1`

Using an Ethernet cable, connect the network interface on the local computer to the management interface on the appliance. Note that the management interface is preconfigured with a default IPv4 address. However, you can reconfigure the management interface with an IPv6 address as part of the setup process.

After initial setup, you can access the console in the following additional ways:

Serial Connection/Laptop

You can connect a computer to any Firepower device using the physical serial port. Connect the appropriate rollover serial cable (also known as a NULL modem cable or Cisco console cable) at any time, then configure the remote management console to redirect the default VGA output to the serial port. To interact with the appliance, use terminal emulation software such as HyperTerminal or XModem. The settings for this software are 9600 baud, 8 data bits, no parity checking, 1 stop bit, and no flow control.

The serial port on a Firepower 8000 Series device uses an RJ-45 connection.

After you connect the appropriate rollover cable to your device, redirect the console output as described in the *Firepower 8000 Series Getting Started Guide*. To locate the serial port for each appliance model, use the diagrams in Hardware Specifications, page 2-1.

Lights-Out Management Using Serial over LAN

The LOM feature allows you to perform a limited set of actions on a Firepower Management Center or Firepower device using a SOL connection. If you need to restore a LOM-capable appliance to factory defaults and do not have physical access to the appliance, you can use LOM to perform the restore process. After you connect to an appliance using LOM, you issue commands to the restore utility as if you were using a physical serial connection. For more information, see the *Firepower 8000 Series Getting Started Guide*.

✎

Note   You can use Lights-Out Management on the default (`eth0`) management interface only.

To use LOM to restore the appliance to factory settings, do **not** delete network settings. Deleting the network settings also drops the LOM connection. For more information, see the *Firepower 8000 Series Getting Started Guide*.

To install the appliance:

Step 1   Mount the appliance in your rack using the mounting kit and its supplied instructions.

Step 2   Connect to the appliance using either a keyboard and monitor or Ethernet connection.

Step 3   If you are using a keyboard and monitor to set up the appliance, use an Ethernet cable now to connect the management interface to a protected network segment.

If you plan to perform the initial setup process by connecting a computer directly to the appliance's management interface, you will connect the management interface to the protected network when you finish setup.

Step 4   For a Firepower device, connect the sensing interfaces to the network segments you want to analyze using the appropriate cables for your interfaces:

- Copper Sensing Interfaces: If your device includes copper sensing interfaces, make sure you use the appropriate cables to connect them to your network; see Cabling Inline Deployments on Copper Interfaces, page 6-5.

- Fiber Adapter Card: For devices with a fiber adapter card, connect the LC connectors on the optional multimode fiber cable to two ports on the adapter card in any order. Connect the SC plug to the network segment you want to analyze.

- Fiber Tap: If you are deploying the device with an optional fiber optic tap, connect the SC plug on the optional multimode fiber cable to the "analyzer" port on the tap. Connect the tap to the network segment you want to analyze.

- Copper Tap: If you are deploying the device with an optional copper tap, connect the A and B ports on the left of the tap to the network segment you want to analyze. Connect the A and B ports on the right of the tap (the "analyzer" ports) to two copper ports on the adapter card.

For more information about options for deploying the managed device, see Deploying Firepower Managed Devices, page 6-1.

Note that if you are deploying a device with bypass interfaces, you are taking advantage of your device's ability to maintain network connectivity even if the device fails. See Testing an Inline Bypass Interface Installation, page 3-18 for information on installation and latency testing.

Step 5   Attach the power cord to the appliance and plug into a power source.

If your appliance has redundant power supplies, attach power cords to both power supplies and plug them into separate power sources.

Step 6   Turn on the appliance.

If you are using a direct Ethernet connection to set up the appliance, confirm that the link LED is on for both the network interface on the local computer and the management interface on the appliance. If the management interface and network interface LEDs are not lit, try using a crossover cable. For more information, see Cabling Inline Deployments on Copper Interfaces, page 6-5.

What To Do Next

- Complete the setup process that allows the new appliance to communicate on your trusted management network; see the *Firepower 8000 Series Getting Started Guide*.

• If you are deploying a device with bypass interfaces, test that you properly installed these devices; see Testing an Inline Bypass Interface Installation, page 3-18.

Testing an Inline Bypass Interface Installation

Managed devices with bypass interfaces provide the ability to maintain network connectivity even when the device is powered off or inoperative. It is important to ensure that you properly install these devices and quantify any latency introduced by their installation.

Note   Your switch's spanning tree discovery protocol can cause a 30-second traffic delay. Cisco recommends that you disable the spanning tree during the following procedure.

The following procedure, applicable only to copper interfaces, describes how to test the installation and ping latency of an inline bypass interface. You will need to connect to the network to run ping tests and connect to the managed device console.

Before You Begin

• Ensure that the interface set type for the Firepower device is configured for inline bypass mode. See Configuring Inline Sets in the *Firepower Management Center Configuration Guide* for instructions on configuring an interface set for inline bypass mode.

To test a device with inline bypass interface installation:

   Access: Admin

Step 1   Set all interfaces on the switch, the firewall, and the device sensing interfaces to auto-negotiate.

Note   Firepower System devices require auto-negotiate when using auto-MDIX on the device.

Step 2   Power off the device and disconnect all network cables.

Reconnect the device and ensure you have the proper network connections. Check cabling instructions for crossover versus straight-through from the device to the switches and firewalls, see Cabling Inline Deployments on Copper Interfaces, page 6-5.

Step 3   With the device powered off, ensure that you can ping from the firewall through the device to the switch.

If the ping fails, correct the network cabling.

Step 4   Run a continuous ping until you complete step 9.

Step 5   Power the device back on.

Step 6   Using your keyboard/monitor or serial connection, log into the device using an account with Administrator privileges. The password is the same as the password for the device's web interface.

The prompt for the device appears.

Step 7   Shut down the device by typing `system shutdown`.

You can also shut down the device using its web interface; see the Managing Devices chapter in the *Firepower Management Center Configuration Guide.* As most devices power off, they emit an audible click sound. The click is the sound of relays switching and the device going into hardware bypass.

Step 8   Wait 30 seconds.

Verify that your ping traffic resumes.

Step 9   Power the device back on, and verify that your ping traffic continues to pass.

Step 10   For Firepower devices that support tap mode, you can test and record ping latency results under the following sets of conditions:

- device powered off
- device powered on, policy with no rules applied, inline intrusion policy protection mode
- device powered on, policy with no rules applied, inline intrusion policy protection tap mode
- device powered on, policy with tuned rules applied, inline intrusion policy protection mode

Ensure that the latency periods are acceptable for your installation. For information on resolving excessive latency problems, see Configuring Packet Latency Thresholding and Understanding Rule Latency Thresholding in the *Firepower Management Center Configuration Guide*.

Using the LCD Panel on a Firepower Device

Firepower devices allow you to view device information or configure certain settings using an LCD panel on the front of the device instead of the system's web interface.

The LCD panel has a display and four multi-function keys, and operates in multiple modes that show different information and allow different configurations depending on the state of the device.

For more information, see the following sections:

- Understanding LCD Panel Components, page 4-2 explains how to identify the components of the LCD panel and display the panel's main menu.
- Using the LCD Multi-Function Keys, page 4-3 explains how to use the multi-function keys on the LCD panel.
- Idle Display Mode, page 4-3 describes how the LCD panel displays various system information when the device is idle.
- Network Configuration Mode, page 4-4 explains how to use the LCD panel to configure the network configuration for the device's management interface: the IPv4 or IPv6 address, subnet mask or prefix, and default gateway.

⚠

Caution Allowing reconfiguration using the LCD panel may present a security risk. You need only physical access, not authentication, to configure using the LCD panel.

- System Status Mode, page 4-6 explains how you can view monitored system information, such as link state propagation, bypass status, and system resources, as well as change the LCD panel brightness and contrast.
- Information Mode, page 4-8 explains how you can view identifying system information such as the device's chassis serial number, IP address, model, and software and firmware versions.
- Error Alert Mode, page 4-9 describes how the LCD panel communicates error or fault conditions; for example, bypass, fan status, or hardware alerts.

✎

Note The device must be powered on to use the LCD panel. For information on how to safely power on or shut down the device, see the Managing Devices chapter in the *Firepower Management Center Configuration Guide*.

Understanding LCD Panel Components

The LCD panel on the front of a Firepower device has a display and four multi-function keys:

- The display contains two lines of text (up to 17 characters each), as well as the multi-function key map. The map indicates, with symbols, the actions that you can perform with the corresponding multi-function keys.

- The multi-function keys allow you to view system information and complete basic configuration tasks, which vary according to the mode of the LCD panel. For more information, see Using the LCD Multi-Function Keys, page 4-3.

The following graphic shows the panel's default Idle Display mode, which does not include a key map.

Figure 4-1   LCD Panel, Idle Display mode

In Idle Display mode, the panel alternates between displaying the CPU utilization and free memory available, and the chassis serial number. Press any key to interrupt the Idle Display mode and enter the LCD panel's main menu where you can access Network Configuration, System Status, and Information modes.

The following graphic shows the main menu, which has a key map that corresponds to the four multi-function keys (top left, top right, bottom left, and bottom right).

Figure 4-2   LCD Panel, main menu
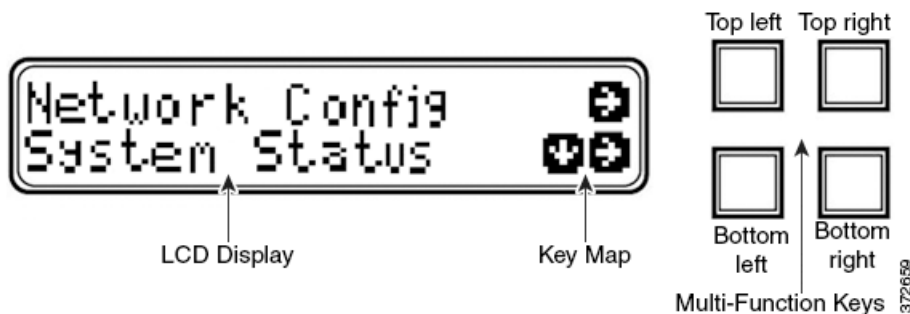
To access the main menu:

Step 1   In Idle Display mode, press any multi-function key.

The main menu appears:

- To change the device's network configuration, see Network Configuration Mode, page 4-4.

- To view monitored system information or adjust the LCD panel brightness and contrast, see System Status Mode, page 4-6.

- To view identifying system information, see Information Mode, page 4-8.

Note   Pressing a multi-function key as the LCD panel enters Idle Display mode can cause the panel to display an unexpected menu.

Using the LCD Multi-Function Keys

Four multi-function keys allow you navigate the menus and options on the LCD panel. You can use the multi-function keys when a key map appears on the display. A symbol's location on the map corresponds to the function and location of the key used to perform that function. If no symbol is displayed, the corresponding key has no function.

Tip   The function of a symbol, and therefore the key map, varies according the LCD panel mode. If you do not get the result you expect, check the mode of the LCD panel.

The following table explains the multi-function key functions.

Table 4-1   LCD Panel Multi-Function Keys

Symbol	Description	Function
↑	Up arrow	Scrolls up the list of current menu options.
↓	Down arrow	Scrolls down the list of current menu options.
←	Left arrow	Performs one of the following actions: • Takes no action and displays the LCD panel menu. • Moves the cursor to the left. • Re-enables editing.
→	Right arrow	Performs one of the following actions: • Enters the menu option displayed on that line. • Moves the cursor to the right. • Scrolls through continued text.
X	Cancel	Cancels the action.
+	Add	Increases the selected digit by one.
-	Subtract	Decreases the selected digit by one.
✓	Check mark	Accepts the action.

Idle Display Mode

The LCD panel enters Idle Display mode after 60 seconds of inactivity (you have not pressed any multi-function keys) with no detected errors. If the system detects an error, the panel enters Error Alert mode (see Error Alert Mode, page 4-9) until the error is resolved. Idle Display mode is also disabled when you are editing your network configuration or running diagnostics.

In Idle Display mode, the panel alternates (at five second intervals) between displaying the CPU utilization and free memory available and the chassis serial number.

A sample of each display might look like this:

```
CPU: 50%
FREE MEM: 1024 MB
```
or:

```
Serial Number:
3D99-101089108-BA0Z
```
In Idle Display mode, press any multi-function key to enter the main menu; see Understanding LCD Panel Components, page 4-2.

Note Pressing a multi-function key as the LCD panel enters Idle Display mode can cause the panel to display an unexpected menu.

Network Configuration Mode

The Firepower System provides a dual stack implementation for both IPv4 and IPv6 management environments. In Network Configuration mode, you can use the LCD panel to configure the network settings for a Firepower device's management interface: the IP address, subnet mask or prefix, and default gateway.

If you edit the IP address of a Firepower device using the LCD panel, confirm that the changes are reflected on the managing Management Center. In some cases, you may need to edit the device management settings manually. See the for more information.

By default, the ability to change network configuration using the LCD panel is disabled. You can enable it during the initial setup process, or using the device's web interface. For more information, see Allowing Network Reconfiguration Using the LCD Panel, page 4-6.

Caution Enabling this option may present a security risk. You need only physical access, not authentication, to configure network settings using the LCD panel.

To configure network settings using Network Configuration mode:

Step 1 In Idle Display mode, press any multi-function key to enter the main menu.

The main menu appears:

```
Network Config         →
System Status        ↓ →
```
Step 2 Press the right arrow (à) key on the top row to access Network Configuration mode.

The LCD panel displays the following:

```
    IPv4                ↓ →

    IPv6                  →
```
Step 3 Press the right arrow key to select the IP address you want to configure:

• For IPv4, the LCD panel might display the following:

```
    IPv4 set to DHCP.   ←

    Enable Manual?      →
```

- For IPv6, the LCD panel might display the following:

  ```
  IPv6 Disabled.      ←

  Enable Manual?      →
  ```

Step 4   Press the right arrow key to manually configure the network:

- For IPv4, the LCD panel displays the IPv4 address. For example:

  ```
  IPv4 Address:     - +

  194.170.001.001   X →
  ```

- For IPv6, the LCD panel displays a blank IPv6 address. For example:

  ```
  IPv6 Address:     - +

  0000:0000:0000:00 X →
  ```

The first line on the panel indicates whether you are editing the IPv4 or IPv6 address. The second line displays the IP address you are editing. A cursor underlines the first digit, and represents the digit you are editing. The two symbols correspond with the multi-function keys to the right of each row.

Note that the IPv6 address does not fit completely on the display. As you edit each digit and move the cursor to the right, the IPv6 address scrolls to the right.

Step 5   Edit the digit underlined by the cursor, if needed, and move to the next digit in the IP address:

- To edit the digit, press the minus (-) or plus (+) keys on the top row to decrease or increase the digit by one.
- To move to the next digit in the IP address, press the right arrow key on the bottom row to move the cursor to the next digit to the right.

With the cursor on the first digit, the LCD panel displays the cancel and right arrow symbols at the end of the IP address. With the cursor on any other digit, the LCD panel displays the left and right arrow symbols.

Step 6   When you finish editing the IPv4 or IPv6 address, press the right arrow key again to display the check mark (✓) key to accept the changes.

Before you press the right arrow key, the function symbols on the display looks like the following sample:

```
IPv4 Address:     - +

194.170.001.001   X →
```

After you press the right arrow key, the function symbols on the display looks like the following sample:

```
IPv4 Address:    X ✓

194.170.001.001     ←
```

Step 7   Press the check mark key to accept the changes to the IP address.

For IPv4, the LCD panel displays the following:

```
Subnet Mask:      - +

000.000.000.000   X →
```

For IPv6, the LCD panel displays the following:

```
Prefix:           - +

000.000.000.000   X →
```

Step 8   Edit the subnet mask or prefix the same way you edited the IP address, and press the check mark key to accept the changes.

The LCD panel displays the following:

```
Default Gateway   - +
000.000.000.000   X →
```

Step 9   Edit the default gateway the same way you edited the IP address, and press the check mark key to accept the changes.

The LCD panel displays the following:

```
Save?               ✓
                    X
```

Step 10   Press the check mark key to save your changes.

Allowing Network Reconfiguration Using the LCD Panel

Because it presents a security risk, the ability to change network configuration using the LCD panel is disabled by default. You can enable it during the initial setup process (see the see the *Firepower 8000 Series Getting Started Guide*), or using the device's web interface as described in the following procedure.

To allow network reconfiguration using a device's LCD panel:

> **Access:** Admin

Step 1   After you complete the initial setup of the device, log into the device's web interface using an account with Administrator privileges.

Step 2   Select **System > Local > Configuration**.

The Information page appears.

Step 3   Click **Network**.

The Network Settings page appears.

Step 4   Under LCD Panel, select the **Allow reconfiguration of network configuration** check box. When the security warning appears, confirm that you want to enable this option.

Tip   For information on the other options on this page, see the *Firepower Management Center Configuration Guide*.

Step 5   Click **Save**.

The network settings are changed.

System Status Mode

The LCD panel's System Status mode displays monitored system information, such as link state propagation, bypass status, and system resources. You can also change the LCD panel's brightness and contrast in System Status mode.

The following table describes the information and options available in this mode.

Table 4-2   System Status Mode Options

Option	Description
Resources	Displays the CPU utilization and free memory available. Note that Idle Display mode also shows this information.

Link State	Displays a list of any inline sets currently in use and the link state status for that set. The first line identifies the inline set, and the second line displays its status (normal or tripped). For example:
	
	`eth2-eth3:`
	`normal`

Fail Open	Displays a list of the bypass inline sets in use and the status of those pairs, either normal or in bypass.
Fan Status	Displays a list and the status of the fans in the device.
Diagnostics	Accessible after pressing a specific key sequence available from Support. ⚠ **Caution** Do **not** access the diagnostics menu without the guidance of Support. Accessing the diagnostics menu without specific instructions from Support can damage your system.
LCD Brightness	Allows you to adjust the brightness of the LCD display.
LCD Contrast	Allows you to adjust the contrast of the LCD display.

To enter System Status mode and view monitored system information:

Step 1   In Idle Display mode, press any multi-function key to enter the main menu.

The main menu appears:

```
Network Config         →
System Status        ↓ →
```

Step 2   Press the right arrow (→) key on the bottom row to access System Status mode.

The LCD panel displays the following:

```
Resources            ↓ →
Link State           ↓ →
```

Step 3   Scroll through the options by pressing the down arrow (â) key. Press the right arrow key in the row next to the status you want to view.

Depending on the option you chose, the LCD panel displays the information listed in Table 4-2 on page 4-7. To change the LCD panel brightness or contrast, see the next procedure.

To adjust the LCD panel brightness or contrast:

Step 1   In System Status mode, scroll through the options by pressing the down arrow (â) key until the LCD panel displays the LCD Brightness and LCD Contrast options:

```
LCD Brightness       ↓ →
```

LCD Contrast   ↓ →

Step 2   Press the right arrow key in the row next to the LCD display feature (brightness or contrast) you want to adjust.

The LCD panel displays the following:

Increase   →
Decrease   ↓ →

Step 3   Press the right arrow key to increase or decrease the display feature you have selected.

The LCD display changes as you press the keys.

Step 4   Press the down arrow to display the Exit option:

Decrease   ↓ →
Exit   →

Step 5   Press the right arrow key in the Exit row to save the setting and return to the main menu.

Information Mode

The LCD panel's Information mode displays identifying system information such as the device's chassis serial number, IP address, model, and software and firmware versions. Support may require this information if you call for assistance.

The following table describes the information available in this mode.

Table 4-3   *Information Mode Options*

Option	Description
IP address	Displays the IP address of the device's management interface.
Model	Displays the device's model.
Serial number	Displays the device's chassis serial number.
Versions	Displays the device's system software and firmware versions. Use the multi-function keys to scroll through the following information: • Product version • NFE version • Micro Engine version • Flash version • GerChr version

To enter Information mode and view identifying system information:

Step 1   In Idle Display mode, press any multi-function key to enter the main menu.

The main menu appears:

Network Config   →
System Status   ↓ →

Step 2   Scroll through the modes by pressing the down arrow (â) key until the LCD panel displays Information mode:

System Status   ↓ →

Information   ↓ →

Step 3   Press the right arrow (→) key on the bottom row to access Information mode.

Step 4   Scroll through the options by pressing the down arrow (â) key. Press the right arrow key in the row next to the information you want to view.

Depending on the option you chose, the LCD panel displays the information listed in Table 4-3 on page 4-8.

Error Alert Mode

When a hardware error or fault condition occurs, Error Alert mode interrupts Idle Display mode. In Error Alert mode, the LCD display flashes and displays one or more of the errors listed in the following table.

Table 4-4   LCD Panel Error Alerts

Error	Description
Hardware alarm	Alerts on hardware alarms
Link state propagation	Displays the link state of paired interfaces
Bypass	Displays the status of inline sets configured in bypass mode
Fan status	Alerts when a fan reaches a critical condition

When a hardware error alert occurs, the LCD displays the main hardware alert menu, as follows:

HARDWARE ERROR!   →
Exit   →

You can use the multi-function keys to scroll through the list of error alerts or exit Error Alert mode. Note that the LCD display continues to flash and display an alert message until all error conditions are resolved.

The LCD panel always displays the platform daemon error message first, followed by a list of other hardware error messages. The following table provides basic information on Firepower device error messages, where *x* indicates the NFE accelerator card (0 or 1) that generated the alert.

Table 4-5   Hardware Alarm Error Messages

Error Message	Condition Monitored	Description
NFE_platformd*X*	platform daemon	Alerts when the platform daemon fails.
NFE_temp*X*	temperature status	Alerts when the temperature of the accelerator card exceeds acceptable limits: • WARNING: greater than 97°C/206°F • CRITICAL: greater than 102°C/215°F
HeartBeat*X*	heartbeat	Alerts when the system cannot detect the heartbeat.
frag*X*	nfe_ipfragd (host frag) daemon	Alerts when the ipfragd daemon fails.
rules*X*	Rulesd (host rules) daemon	Alerts when the Rulesd daemon fails.
TCAM*X*	TCAM daemon	Alerts when the TCAM daemon fails.

Table 4-5   Hardware Alarm Error Messages (continued)

Error Message	Condition Monitored	Description
NFEMessD*X*	message daemon	Alerts when the message daemon fails.
NFEHardware	hardware status	Alerts when one or more accelerator cards is not communicating.
NFEcount	cards detected	Alerts when the number of accelerator cards detected on the device does not match the expected accelerator card count for the platform.
NMSB_comm	communications	Alerts when the media assembly is not present or not communicating.
scmd	scmd daemon status	Alerts when the scmd daemon fails.
psls	psls daemon status	Alerts when the psls daemon fails.
ftwo	ftwo daemon status	Alerts when the ftwo daemon fails.
NFE_port18 NFE_port19 NFE_port20 NFE_port21	internal link status	Alerts when the link between the network module switch board and the accelerator card fails: • 81xx Family: NFE_port18 and NFE_port19 only 82xx Family and 83xx Family: NFE_port18, NFE_port19, NFE_port20, and NFE_port21

Use the following procedure to view hardware alert error messages on the LCD display.

To view the hardware alert error messages:

Step 1 In Error Alert mode, on the HARDWARE ERROR! line, press the right arrow (→) key to view the hardware errors that triggered the Error Alert mode.

The LCD panel lists the error alert messages starting with the NFE platform daemon failure followed by a list of error messages.

    NFEplatformd*X*
    NFEtemp*X*   ↓
where *X* indicates the accelerator card (either 0 or 1) that generated the alert.

Step 2 On the error message line, press the down arrow (â) key to view additional errors. When there are no additional errors, the Exit row appears.

    Exit   →
Step 3 Press the right arrow (→) key to exit Error Alert mode.

If you exit Error Alert mode before you resolve the error that triggered the alert, the LCD panel returns to Error Alert mode. Contact Support for assistance.

CHAPTER **5**

Deploying on a Management Network

The Firepower System can be deployed to accommodate the needs of each unique network architecture. The Management Center provides a centralized management console and database repository for the Firepower System. Devices are installed on network segments to collect traffic connections for analysis.

Management Centers use a management interface to connect to a *trusted management network* (that is, a secure internal network not exposed external traffic). Devices connect to a Management Center using a management interface.

Devices then connect to an external network using sensing interfaces to monitor traffic. For more information on how to use sensing interfaces in your deployment, see Deploying Firepower Managed Devices, page 6-1.

Management Deployment Considerations

Your management deployment decisions are based on a variety of factors. Answering these questions can help you understand your deployment options to configure the most efficient and effective system:

- Will you use the default single management interface to connect your device to your Management Center? Will you enable additional management interfaces to improve performance, or to isolate traffic received on the Management Center from different networks? See Understanding Management Interfaces, page 5-2 for more information.

- Do you want to enable traffic channels to create two connections between the Management Center and the managed device to improve performance? Do you want to use multiple management interfaces to further increase throughput capacity between the Management Center and the managed device? See Deploying with Traffic Channels, page 5-3 for more information.

- Do you want to use one Management Center to manage and isolate traffic from devices on different networks? See Deploying with Network Routes, page 5-4 for more information.

- Are you deploying your management interfaces in a protected environment? Is appliance access restricted to specific workstation IP addresses? Security Considerations, page 5-5 describes considerations for deploying your management interfaces securely.

- Are you deploying 8000 Series devices? See Special Case: Connecting 8000 Series Devices, page 5-5 for more information.

Understanding Management Interfaces

Management interfaces provide the means of communication between the Management Center and all devices it manages. Maintaining good traffic control between the appliances is essential to the success of your deployment.

On Management Centers and Firepower devices, you can enable the management interface on the Management Center, device, or both, to sort traffic between the appliances into two separate traffic channels. The *management traffic channel* carries all internal traffic (that is, inter-device traffic specific to the management of the appliance and the system), and the *event traffic channel* carries all event traffic (that is, high volume event traffic, such as intrusion and malware events). Splitting traffic into two channels creates two connection points between the appliances which increases throughput, thus improving performance. You can also enable *multiple management interfaces* to provide still greater throughput between appliances, or to manage and isolate traffic between devices on different networks.

After you register the device to the Management Center, you can change the default configuration to enable traffic channels and multiple management interfaces using the web interface on each appliance. For configuration information, see Configuring Appliance Settings in the *Firepower Management Center Configuration Guide*.

Management interfaces are often located on the back of the appliance. See Identifying the Management Interfaces, page 3-2 for more information.

Single Management Interface

When you register your device to a Management Center, you establish a single communication channel that carries all traffic between the management interface on the Management Center and the management interface on the device.

The following graphic shows the default single communication channel. One interface carries one communication channel that contains both management and event traffic.

Multiple Management Interfaces

You can enable and configure multiple management interfaces, each with a specific IPv4 or IPv6 address and, optionally, a hostname, to provide greater traffic throughput by sending each traffic channel to a different management interface. Configure a smaller interface to carry the lighter management traffic load, and a larger interface to carry the heavier event traffic load. You can register devices to separate management interfaces and configure both traffic channels for the same interface, or use a dedicated management interface to carry the event traffic channels for all devices managed by the Management Center.

You can also create a route from a specific management interface on your Management Center to a different network, allowing your Management Center to isolate and manage device traffic on one network separately from device traffic on another network.

Additional management interfaces function the same as the default management interface with the following exceptions:

- You can configure DHCP on the default (`eth0`) management interface only. Additional (`eth1` and so on) interfaces require unique static IP addresses and hostnames. Cisco recommends that you do not set up DNS entries for additional management interfaces but instead register Management Centers and devices by IP addresses only for these interfaces.

- You must configure both traffic channels to use the same management interface when you use a non-default management interface to connect your Management Center and managed device and those appliances are separated by a NAT device.

- You can use Lights-Out Management on the default management interface only.

- On the 70xx Family, you can separate traffic into two channels and configure those channels to send traffic to one or more management interfaces on the Management Center. However, because the 70xx Family contains only one management interface, the device receives traffic sent from the Management Center on only one management interface.

Deployment Options

You can manage traffic flow using traffic channels to improve performance on your system using one or more management interfaces. In addition, you can create a route to a different network using a specific management interface on the Management Center and its managed device, allowing you to isolate traffic between devices on different networks. For more information, see the following sections:

Deploying with Traffic Channels

When you use two traffic channels on one management interface, you create two connections between the Management Center and the managed device. One channel carries management traffic and one carries event traffic, separately and on the same interface.

The following example shows the communication channel with two separate traffic channels on the same interface.
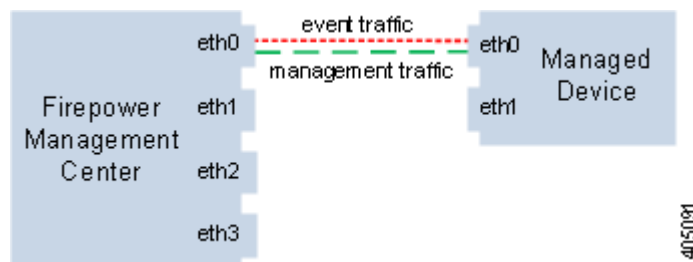
When you use multiple management interfaces, you can improve your performance by dividing the traffic channels over two management interfaces, thus increasing the traffic flow by adding the capacity of both interfaces. One interface carries the management traffic channel and the other carries the event traffic channel. If either interface fails, all traffic reroutes to the active interface and the connection is maintained.

The following graphic shows the management traffic channel and the event traffic channel over two management interfaces.

You can use a dedicated management interface to carry only event traffic from multiple devices. In this configuration, each device is registered to a different management interface to carry the management traffic channel, and one management interface on the Management Center carries all event traffic channels from all devices. If an interface fails, traffic reroutes to the active interface and the connection is maintained. Note that because event traffic for all devices is carried on the same interface, traffic is not isolated between networks.

The following graphic shows two devices using different management channel traffic interfaces sharing the same dedicated interface for event traffic channels.
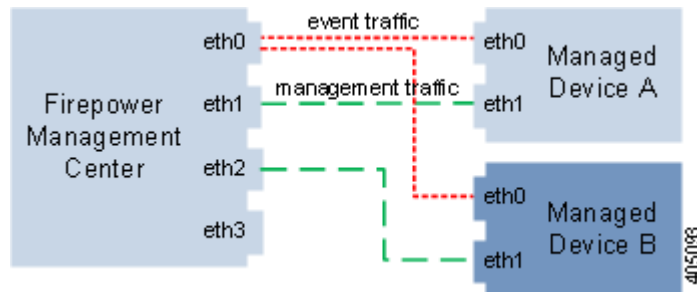
Deploying with Network Routes

You can create a route from a specific management interface on your Management Center to a different network. When you register a device from that network to the specified management interface on the Management Center, you provide an isolated connection between the Management Center and the device on a different network. Configure both traffic channels to use the same management interface to ensure that traffic from that device remains isolated from device traffic on other networks. Because the routed interface is isolated from all other interfaces on the Management Center, if the routed management interface fails, the connection is lost.

**Tip**   You must register a device to the static IP address of any management interface other than the default (eth0) management interface. DHCP is supported only on the default management interface.

After you install your Management Center, you configure multiple management interfaces using the web interface. See Configuring Appliance Settings in the *Firepower Management Center Configuration Guide* for more information.

The following graphic shows two devices isolating network traffic by using separate management interfaces for all traffic. You can add more management interfaces to configure separate management and event traffic channel interfaces for each device.
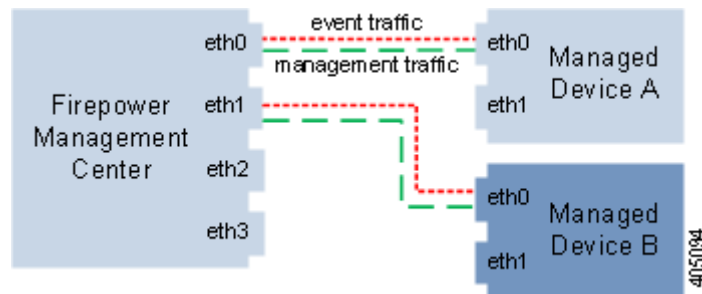
Security Considerations

To deploy your management interfaces in a secure environment, Cisco recommends that you consider the following:

- Always connect the management interface to a trusted internal management network that is protected from unauthorized access.

- Identify the specific workstation IP addresses that can be allowed to access appliances. Restrict access to the appliance to only those specific hosts using Access Lists within the appliance's system policy. For more information, see the *Firepower Management Center Configuration Guide*.

Special Case: Connecting 8000 Series Devices

Supported Devices: 8000 Series

When you register an 8000 Series device to your Management Center, you must either auto-negotiate on both sides of the connection, or set both sides to the same static speed to ensure a stable network link. 8000 Series devices do not support half duplex network links; they also do not support differences in speed or duplex configurations at opposite ends of a connection.

Deploying Firepower Managed Devices

After you register a device to a Firepower Management Center, you deploy the sensing interfaces of the device on a network segment to monitor traffic using an intrusion detection system or protect your network from threats using an intrusion prevention system.

Sensing Deployment Considerations

Your sensing deployment decisions will be based on a variety of factors. Answering these questions can help you understand the vulnerable areas of your network and clarify your intrusion detection and prevention needs:

- Will you be deploying your managed device with passive or inline interfaces? Does your device support a mix of interfaces, some passive and others inline? See Understanding Sensing Interfaces, page 6-1 for more information.

- How will you connect the managed devices to the network? Hubs? Taps? Spanning ports on switches? Virtual switches? See Connecting Devices to Your Network, page 6-4 for more information.

- Do you want to detect every attack on your network, or do you only want to know about attacks that penetrate your firewall? Do you have specific assets on your network such as financial, accounting, or personnel records, production code, or other sensitive, protected information that require special security policies? See Deployment Options, page 6-7 for more information.

- Will you use multiple sensing interfaces on your managed device to recombine the separate connections from a network tap, or to capture and evaluate traffic from different networks? Do you want to use the multiple sensing interfaces to perform as a virtual router or a virtual switch? See Using Multiple Sensing Interfaces on a Managed Device, page 6-16 for more information.

- Do you provide VPN or modem access for remote workers? Do you have remote offices that also require an intrusion protection deployment? Do you employ contractors or other temporary employees? Are they restricted to specific network segments? Do you integrate your network with the networks of other organizations such as customers, suppliers, or business partners? See Complex Network Deployments, page 6-18 for more information.

Understanding Sensing Interfaces

The sections that follow describe how different sensing interfaces affect the capabilities of the Firepower System. In addition to passive and inline interfaces, you can also have routed, switched, and hybrid interfaces.

Sensing interfaces are located on the front of the device. To identify your sensing interfaces, see Identifying the Sensing Interfaces, page 3-3.

Passive Interfaces

You can configure a passive deployment to monitor traffic flowing across a network using a switch SPAN, virtual switch, or mirror port, allowing traffic to be copied from other ports on the switch. Passive interfaces allow you to inspect traffic within the network without being in the flow of network traffic. When configured in a passive deployment, the system cannot take certain actions such as blocking or shaping traffic. Passive interfaces receive all traffic unconditionally and do not retransmit received traffic.

Inline Interfaces

You configure an inline deployment transparently on a network segment by binding two ports together. Inline interfaces allow you to install a device in any network configuration without the configuration of adjacent network devices. Inline interfaces receive all traffic unconditionally, then retransmit all traffic received on these interfaces except traffic explicitly dropped. You must assign a pair of inline interfaces to an inline set before they can handle traffic in an inline deployment.

Note   If you configure an interface as an inline interface, the adjacent port on its NetMod automatically becomes an inline interface as well to complete the pair.

Configurable bypass inline sets allow you to select how your traffic is handled if your hardware fails completely (for example, the device loses power). You may determine that connectivity is critical on one network segment, and, on another network segment, you cannot permit uninspected traffic. Using configurable bypass inline sets, you can manage the traffic flow of your network traffic in one of the following ways:

- *Bypass*: an interface pair configured for bypass allows all traffic to flow if the device fails. The traffic bypasses the device and any inspection or other processing by the device. Bypass allows uninspected traffic across the network segment, but ensures that the network connectivity is maintained.

- *Non-bypass*: an interface pair configured for non-bypass stops all traffic if the device fails. Traffic that reaches the failed device does not enter the device. Non-bypass does not permit traffic to pass uninspected, but the network segment loses connectivity if the device fails. Use non-bypass interfaces in deployment situations where network security is more important than loss of traffic.

Configure the inline set as bypass to ensure that traffic continues to flow if your device fails. Configure the inline set as non-bypass to stop traffic if the device fails. Note that reimaging resets Firepower devices in bypass mode to a non-bypass configuration and disrupts traffic on your network until you reconfigure bypass mode. For more information, see the see the *Firepower 8000 Series Getting Started Guide*.

All Firepower devices can contain configurable bypass interfaces. 8000 Series devices can also contain NetMods with interfaces that cannot be configured for bypass. For more information on NetMods, see Firepower 8000 Series Modules, page 2-13. Other advanced interface options include tap mode, propagate link state, transparent inline mode, and strict TCP mode. For information on how to configure your inline interface sets, see Configuring Inline Sets in the *Firepower Management Center Configuration Guide*. For more information on using inline interfaces, see Connecting Devices to Your Network, page 6-4.

You cannot configure bypass interfaces on an ASA FirePOWER device using the Firepower Management Center. For information on configuring an ASA FirePOWER device in inline mode, see the ASA documentation.

Switched Interfaces

You can configure switched interfaces on a Firepower device in a Layer 2 deployment to provide packet switching between two or more networks. You can also configure virtual switches on Firepower devices to operate as standalone broadcast domains, dividing your network into logical segments. A virtual switch uses the media access control (MAC) address from a host to determine where to send packets.

Switched interfaces can have either a physical or logical configuration:

- *Physical switched interfaces* are physical interfaces with switching configured. Use physical switched interfaces to handle untagged VLAN traffic.

- *Logical switched interfaces* are an association between a physical interface and a VLAN tag. Use logical interfaces to handle traffic with designated VLAN tags.

Virtual switches can operate as standalone broadcast domains, dividing your network into logical segments. A virtual switch uses the media access control (MAC) address from a host to determine where to send packets. When you configure a virtual switch, the switch initially broadcasts packets through every available port on the switch. Over time, the switch uses tagged return traffic to learn which hosts reside on the networks connected to each port.

You can configure your device as a virtual switch and use the remaining interfaces to connect to network segments you want to monitor. To use a virtual switch on your device, create physical switched interfaces and then follow the instructions for Setting Up Virtual Switches in the *Firepower Management Center Configuration Guide*.

Routed Interfaces

You can configure routed interfaces on a Firepower device in a Layer 3 deployment so that it routes traffic between two or more interfaces. You must assign an IP address to each interface and assign the interfaces to a virtual router to route traffic.

You can configure routed interfaces for use with a gateway virtual private network (gateway VPN) or with network address translation (NAT). For more information, see Deploying a Gateway VPN, page 6-10 and Deploying with Policy-Based NAT, page 6-11.

You can also configure the system to route packets by making packet forwarding decisions according to the destination address. Interfaces configured as routed interfaces receive and forward the Layer 3 traffic. Routers obtain the destination from the outgoing interface based on the forwarding criteria, and access control rules designate the security policies to be applied.

Routed interfaces can have either a physical or logical configuration:

- *Physical routed interfaces* are physical interfaces with routing configured. Uses physical routed interfaces to handle untagged VLAN traffic.

- *Logical switched interfaces* are an association between a physical interface and a VLAN tag. Use logical interfaces to handle traffic with designated VLAN tags.

To use routed interfaces in a Layer 3 deployment, you must configure virtual routers and assign routed interfaces to them. A virtual router is a group of routed interfaces that route Layer 3 traffic.

You can configure your device as a virtual router and use the remaining interfaces to connect to network segments you want to monitor. You can also enable strict TCP enforcement for maximum TCP security. To use a virtual router on your device, create physical routed interfaces on your device and then follow the instructions for Setting Up Virtual Routers in the *Firepower Management Center Configuration Guide*.

Hybrid Interfaces

You can configure logical hybrid interfaces on Firepower devices that allow the Firepower System to bridge traffic between virtual routers and virtual switches. If IP traffic received on interfaces in a virtual switch is addressed to the MAC address of an associated hybrid logical interface, the system handles it as Layer 3 traffic and either routes or responds to the traffic depending on the destination IP address. If the system receives any other traffic, it handles it as Layer 2 traffic and switches it appropriately.

To create a hybrid interface, you first configure a virtual switch and virtual router, then add the virtual switch and virtual router to the hybrid interface. A hybrid interface that is not associated with both a virtual switch and a virtual router is not available for routing, and does not generate or respond to traffic.

You can configure hybrid interfaces with network address translation (NAT) to pass traffic between networks. For more information, see Deploying with Policy-Based NAT, page 6-11.

If you want to use hybrid interfaces on your device, define a hybrid interface on the device and then follow the instructions for Setting Up Hybrid Interfaces in the *Firepower Management Center Configuration Guide*.

Connecting Devices to Your Network

You can connect the sensing interfaces on your managed devices to your network in several ways. Configure a hub or network tap using either passive or inline interfaces, or a span port using passive interfaces.

Using a Hub

An Ethernet hub is a simple way to ensure that the managed device can see all the traffic on a network segment. Most hubs of this type take the IP traffic meant for any of the hosts on the segment and broadcast it to all the devices connected to the hub. Connect the interface set to the hub to monitor all incoming and outgoing traffic on the segment. Using a hub does not guarantee that the detection engine sees every packet on a higher volume network because of the potential of packet collision. For a simple network with low traffic, this is not likely to be a problem. In a high-traffic network, a different option may provide better results. Note that if the hub fails or loses power, the network connection is broken. In a simple network, the network would be down.

Some devices are marketed as hubs but actually function as switches and do not broadcast each packet to every port. If you attach your managed device to a hub, but do not see all the traffic, you may need to purchase a different hub or use a switch with a Span port.

Using a Span Port

Many network switches include a span port that mirrors traffic from one or more ports. By connecting an interface set to the span port, you can monitor the combined traffic from all ports, generally both incoming and outgoing. If you already have a switch that includes this feature on your network, in the proper location, then you can deploy the detection on multiple segments with little extra equipment cost beyond the cost of the managed device. In high-traffic networks, this solution has its limitations. If the span port can handle 200Mbps and each of three mirrored ports can handle up to 100Mbps, then the span port is likely to become oversubscribed and drop packets, lowering the effectiveness of the managed device.

Using a Network Tap

Network taps allow you to passively monitor traffic without interrupting the network flow or changing the network topology. Taps are readily available for different bandwidths and allow you to analyze both incoming and outgoing packets on a network segment. Because you can monitor only a single network segment with most taps, they are not a good solution if you want to monitor the traffic on two of the eight ports on a switch. Instead, you would install the tap between the router and the switch and access the full IP stream to the switch.

By design, network taps divide incoming and outgoing traffic into two different streams over two different cables. Managed devices offer multiple sensing interface options that recombine the two sides of the conversation so that the entire traffic stream is evaluated by the decoders, the preprocessors, and the detection engine.

Cabling Inline Deployments on Copper Interfaces

If you deploy your device inline on your network and you want to use your device's bypass capabilities to maintain network connectivity if the device fails, you must pay special attention to how you cable the connections.

If you deploy a device with fiber bypass capable interfaces, there are no special cabling issues beyond ensuring that the connections are securely fastened and the cables are not kinked. However, if you are deploying devices with copper rather than fiber network interfaces, then you must be aware of the device model that you are using, because different device models use different network cards. Note that some 8000 Series NetMods do not allow bypass configuration.

The network interface cards (NICs) in the device support a feature called Auto-Medium Dependent Interface Crossover (Auto-MDI-X), which allows network interfaces to configure automatically whether you use a straight-through or crossover Ethernet cable to connect to another network device. Firepower devices bypass as crossover connections.

Wire the device as would normally be done without a device deployed. The link should work with power to the device removed. In most cases you should use two straight-through cables to connect the device to the two endpoints.

Figure 6-1   Crossover Bypass Connection Cabling

The following table indicates where you should use crossover or straight-through cables in your hardware bypass configurations. Note that a Layer 2 port functions as a straight-through (MDI) endpoint in the deployment, and a Layer 3 port functions as a crossover (MDIX) endpoint in the deployment. The total crossovers (cables and appliances) should be an odd number for bypass to function properly.

Table 6-1   Valid Configurations for Hardware Bypass

Endpoint 1	Cable	Managed Device	Cable	Endpoint 2
MDIX	straight-through	straight-through	straight-through	MDI
MDI	crossover	straight-through	straight-through	MDI
MDI	straight-through	straight-through	crossover	MDI
MDI	straight-through	straight-through	straight-through	MDIX
MDIX	straight-through	crossover	straight-through	MDIX
MDI	straight-through	crossover	straight-through	MDI
MDI	crossover	crossover	crossover	MDI
MDIX	crossover	crossover	straight-through	MDI

Note that every network environment is likely to be unique, with endpoints that have different combinations of support for Auto-MDI-X. The easiest way to confirm that you are installing your device with the correct cabling is to begin by connecting the device to its two endpoints using one crossover cable and one straight-through cable, but with the device powered down. Ensure that the two endpoints can communicate. If they cannot communicate, then one of the cables is the incorrect type. Switch one (and only one) of the cables to the other type, either straight-through or crossover.

After the two endpoints can successfully communicate with the inline device powered down, power up the device. The Auto-MDI-X feature ensures that the two endpoints will continue to communicate. Note that if you have to replace an inline device, you should repeat the process of ensuring that the endpoints can communicate with the new device powered down to protect against the case where the original device and its replacement have different bypass characteristics.

The Auto-MDI-X setting functions correctly only if you allow the network interfaces to auto-negotiate. If your network environment requires that you turn off the Auto Negotiate option on the Network Interface page, then you must specify the correct MDI/MDIX option for your inline network interfaces. See Configuring Inline Interfaces in the *Firepower Management Center Configuration Guide* for more information.

Special Case: Connecting Firepower 8000 Series Devices

When you register a Firepower 8000 Series managed device to your Firepower Management Center, you must either use auto-negotiation on both sides of the connection, or set both sides to the same static speed to ensure a stable network link. 8000 Series managed devices do not support half duplex network links; they also do not support differences in speed or duplex configurations at opposite ends of a connection.

Deployment Options

When you place your managed device on a network segment, you can monitor traffic using an intrusion detection system or protect your network from threats using an intrusion prevention system.

You can also deploy your managed device to function as a virtual switch, virtual router, or gateway VPN. Additionally, you can use policies to route traffic or control access to traffic on your network.

Deploying with a Virtual Switch

You can create a *virtual switch* on your managed device by configuring inline interfaces as switched interfaces. The virtual switch provides Layer 2 packet switching for your deployment. Advanced options include setting a static MAC address, enabling spanning tree protocol, enabling strict TCP enforcement, and dropping bridge protocol data units (BPDUs) at the domain level. For information on switched interfaces, see Switched Interfaces, page 6-3.

A virtual switch must contain two or more switched interfaces to handle traffic. For each virtual switch, the system switches traffic only to the set of ports configured as switched interfaces. For example, if you configure a virtual switch with four switched interfaces, when the system receives traffic packets through one port it only broadcasts these packets to the remaining three ports on the switch.

To configure a virtual switch to allow traffic, you configure two or more switched interfaces on a physical port, add and configure a virtual switch, and then assign the virtual switch to the switched interfaces. The system drops any traffic received on an external physical interface that does not have a switched interface waiting for it. If the system receives a packet with no VLAN tag and you have not configured a physical switched interface for that port, it drops the packet. If the system receives a VLAN-tagged packet and you have not configured a logical switched interface, it also drops the packet.

You can define additional logical switched interfaces on the physical port as needed, but you must assign a logical switched interface to a virtual switch to handle traffic.

Virtual switches have the advantage of scalability. When you use a physical switch, you are limited by the number of available ports on the switch. When you replace your physical switch with a virtual switch, you are limited only by your bandwidth and the level of complexity you want to introduce to your deployment.

Use a virtual switch where you would use a Layer 2 switch, such as workgroup connectivity and network segmentation. Layer 2 switches are particularly effective where workers spend most of their time on their local segment. Larger deployments (for example, deployments that contain broadcast traffic, Voice-over-IP, or multiple networks) can use virtual switches on smaller network segments of the deployment.

When you deploy multiple virtual switches on the same managed device, you can maintain separate levels of security as dictated by the needs of each network.

Figure 6-2   *Virtual Switches on a Managed Device*
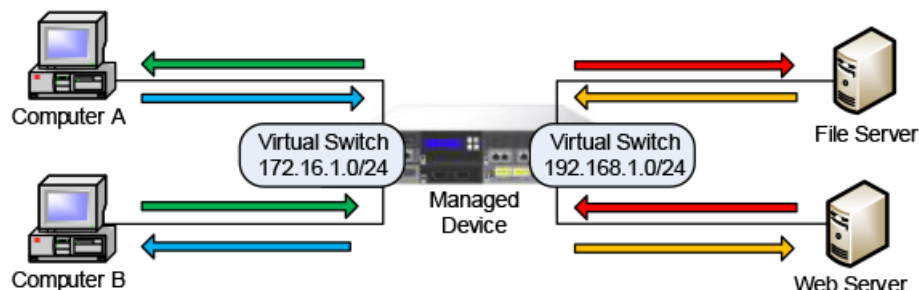
In this example, the managed device monitors traffic from two separate networks, 172.16.1.0/20 and 192.168.1.0/24. Although both networks are monitored by the same managed device, the virtual switch passes traffic only to those computers or servers on the same network. Traffic can pass from computer A to computer B through the 172.16.1.0/24 virtual switch (indicated by the blue line) and from computer B to computer A through the same virtual switch (indicated by the green line). Similarly, traffic can pass to and from the file and web servers through the 192.168.1.0/24 virtual switch (indicated by the red and orange lines). However, traffic cannot pass between the computers and the web or file servers because the computers are not on the same virtual switch as the servers.

For more information on configuring switched interfaces and virtual switches, see Setting Up Virtual Switches in the *Firepower Management Center Configuration Guide.*

Deploying with a Virtual Router

You can create a *virtual router* on a managed device to route traffic between two or more networks, or to connect a private network to a public network (for example, the Internet). The virtual router connects two routed interfaces to provide Layer 3 packet forwarding decisions for your deployment according to the destination address. Optionally, you can enable strict TCP enforcement on the virtual router. For more information on routed interfaces, see Routed Interfaces, page 6-3. You must use a virtual router with a gateway VPN. For more information, see Deploying a Gateway VPN, page 6-10.

A virtual router can contain either physical or logical routed configurations from one or more individual devices within the same broadcast domain. You must associate each logical interface with a VLAN tag to handle traffic received by the physical interface with that specific tag. You must assign a logical routed interface to a virtual router to route traffic.

To configure a virtual router, you set up routed interfaces with either physical or logical configurations. You can configure physical routed interfaces for handling untagged VLAN traffic. You can also create logical routed interfaces for handling traffic with designated VLAN tags. The system drops any traffic received on an external physical interface that does not have a routed interface waiting for it. If the system receives a packet with no VLAN tag and you have not configured a physical routed interface for that port, it drops the packet. If the system receives a VLAN-tagged packet and you have not configured a logical routed interface, it also drops the packet.

Virtual routers have the advantage of scalability. Where physical routers limit the number of networks you can connect, multiple virtual routers can be configured on the same managed device. Putting multiple routers on the same device reduces the physical complexity of your deployment, allowing you to monitor and manage multiple routers from one device.

Use a virtual router where you would use a Layer 3 physical router to forward traffic between multiple networks in your deployment, or to connect your private network to a public network. Virtual routers are particularly effective in large deployments where you have many networks or network segments with different security requirements.

When you deploy a virtual router on your managed device, you can use one appliance to connect multiple networks to each other, and to the Internet.

Figure 6-3   *Virtual Routers on a Managed Device*
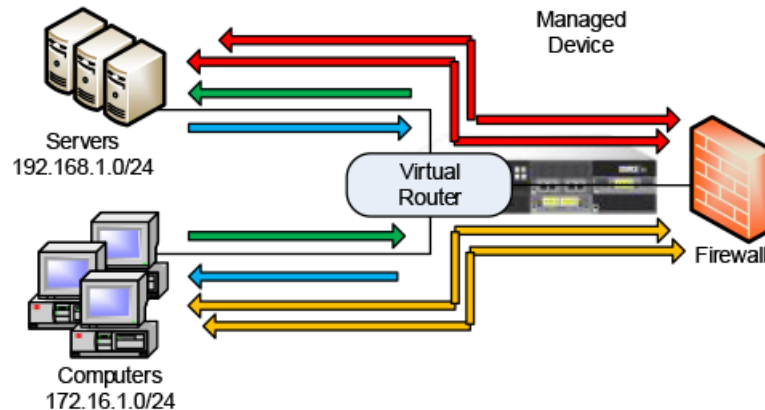
In this example, the managed device contains a virtual router to allow traffic to travel between the computers on network 172.16.1.0/20 and the servers on network 192.168.1.0/24 (indicated by the blue and green lines). A third interface on the virtual router allows traffic from each network to pass to the firewall and back (indicated by the red and orange lines).

For more information, see Setting Up Virtual Routers in the *Firepower Management Center Configuration Guide*.

Deploying with Hybrid Interfaces

You can create a *hybrid interface* on a managed device to route traffic between Layer 2 and Layer 3 networks using a virtual switch and a virtual router. This provides one interface that can both route local traffic on the switch and route traffic to and from an external network. For best results, configure policy-based NAT on the interface to provide network address translation on the hybrid interface. See Deploying with Policy-Based NAT, page 6-11.

A hybrid interface must contain one or more switched interfaces and one or more routed interfaces. A common deployment consists of two switched interfaces configured as a virtual switch to pass traffic on a local network and virtual routers to route traffic to networks, either private or public.
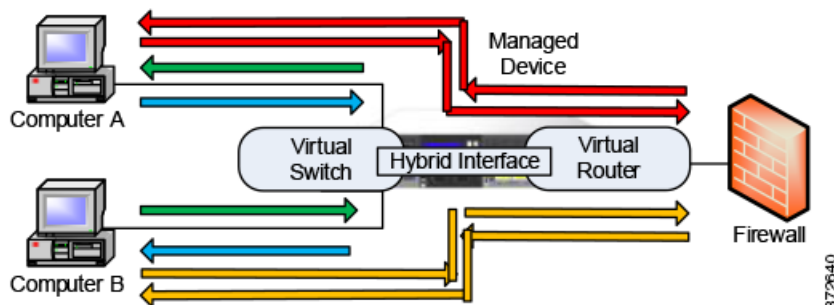
To create a hybrid interface, you first configure a virtual switch and virtual router, then add the virtual switch and virtual router to the hybrid interface. A hybrid interface that is not associated with both a virtual switch and a virtual router is not available for routing, and does not generate or respond to traffic.

Hybrid interfaces have the advantage of compactness and scalability. Using a single hybrid interface combines both Layer 2 and Layer 3 traffic routing functions in a single interface, reducing the number of physical appliances in the deployment and providing a single management interface for the traffic.

Use a hybrid interface where you need both Layer 2 and Layer 3 routing functions. This deployment can be ideal for small segments of your deployment where you have limited space and resources.

When you deploy a hybrid interface, you can allow traffic to pass from your local network to an external or public network, such as the Internet, while addressing separate security considerations for the virtual switch and virtual router in the hybrid interface.

Figure 6-4   Hybrid Interface on a Managed Device

In this example, computer A and computer B are on the same network and communicate using a Layer 2 virtual switch configured on the managed device (indicated by the blue and green lines). A virtual router configured on the managed device provides Layer 3 access to the firewall. A hybrid interface combines the Layer 2 and Layer 3 capabilities of the virtual switch and virtual router to allow traffic to pass from each computer through the hybrid interface to the firewall (indicated by the red and orange lines).

For more information, see Setting Up Hybrid Interfaces in the *Firepower Management Center Configuration Guide*.

Deploying a Gateway VPN

License: VPN

You can create a *gateway virtual private network* (gateway VPN) connection to establish a secure tunnel between a local gateway and a remote gateway. The secure tunnel between the gateways protects communication between them.

You configure the Firepower System to build secure VPN tunnels from the virtual routers of Cisco managed devices to remote devices or other third-party VPN endpoints using the Internet Protocol Security (IPSec) protocol suite. After the VPN connection is established, the hosts behind the local gateway can connect to the hosts behind the remote gateway through the secure VPN tunnel. The VPN endpoints authenticate each other with either the Internet Key Exchange (IKE) version 1 or version 2 protocol to create a security association for the tunnel. The system runs in either IPSec authentication header (AH) mode or the IPSec encapsulating security payload (ESP) mode. Both AH and ESP provide authentication, and ESP also provides encryption.

A gateway VPN can be used in a point-to-point, star, or mesh deployment:

- Point-to-point deployments connect two endpoints with each other in a direct one-to-one relationship. Both endpoints are configured as peer devices, and either device can initiate the secured connection. At least one device must be a VPN-enabled managed device.

  Use a point-to-point deployment to maintain your network security when a host at a remote location uses public networks to connect to a host in your network.

- Star deployments establish a secure connection between a hub and multiple remote endpoints (leaf nodes). Each connection between the hub node and an individual leaf node is a separate VPN tunnel. Typically, the hub node is the VPN-enabled managed device, located at the main office. Leaf nodes are located at branch offices and initiate most of the traffic.

  Use a star deployment to connect an organization's main and branch office locations using secure connections over the Internet or other third-party network to provide all employees with controlled access to the organization's network.

- Mesh deployments connect all endpoints together by means of VPN tunnels. This offers redundancy in that when one endpoint fails, the remaining endpoints can still communicate with each other.

  Use a mesh deployment to connect a group of decentralized branch office locations to ensure that traffic can travel even if one or more VPN tunnels fails. The number of VPN-enabled managed devices you deploy in this configuration controls the level of redundancy.

For more information on gateway VPN configuration and deployments, see Gateway VPN in the *Firepower Management Center Configuration Guide*.

Deploying with Policy-Based NAT

You can use *policy-based network address translation* (NAT) to define policies that specify how you want to perform NAT. You can target your policies to a single interface, one or more devices, or entire networks.

You can configure static (one-to-one) or dynamic (one-to-many) translation. Note that dynamic translations are order-dependent where rules are searched in order until the first matching rule applies.

Policy-based NAT typically operates in the following deployments:

- Hide your private network address.

  When you access a public network from your private network, NAT translates your private network address to your public network address. Your specific private network address is hidden from the public network.

- Allow access to a private network service.

  When a public network accesses your private network, NAT translates your public address to your private network address. The public network can access your specific private network address.

- Redirect traffic between multiple private networks.

  When a server on a private network accesses a server on a connected private network, NAT translates the private addresses between the two private networks to ensure there is no duplication in private addresses and traffic can travel between them.

Using policy-based NAT removes the need for additional hardware and consolidates the configuration of your intrusion detection or prevention system and NAT into a single user interface. For more information, see Using NAT Policies in the *Firepower Management Center Configuration Guide*.

Deploying with Access Control

Access control is a policy-based feature that allows you to specify, inspect, and log the traffic that can enter, exit, or travel within your network. The following section describes how access control can function in your deployment. See the *Firepower Management Center Configuration Guide* for more information on this feature.

An access control policy determines how the system handles traffic on your network. You can add access control rules to your policy to provide more granular control over how you handle and log network traffic.

An access control policy that does not include access control rules uses one of the following default actions to handle traffic:

- block all traffic from entering your network
- trust all traffic to enter your network without further inspection

- allow all traffic to enter your network, and inspect the traffic with a network discovery policy only

- allow all traffic to enter your network, and inspect the traffic with intrusion and network discovery policies

Access control rules further define how traffic is handled by targeted devices, from simple IP address matching to complex scenarios involving different users, applications, ports, and URLs. For each rule, you specify a rule action, that is, whether to trust, monitor, block, or inspect matching traffic with an intrusion or file policy.

Access control can filter traffic based on Security Intelligence data, a feature that allows you to specify the traffic that can traverse your network, per access control policy, based on the source or destination IP address. This feature can create a blacklist of disallowed IP addresses whose traffic is blocked and not inspected.

The sample deployment illustrates common network segments. Deploying your managed devices in each of these locations serves different purposes. The following sections describe typical location recommendations:

- Inside the Firewall, page 6-12 explains how access control functions on traffic that passes through the firewall.

- On the DMZ, page 6-13 explains how access control within the DMZ can protect outward-facing servers.

- On the Internal Network, page 6-14 explains how access control can protect your internal network from intentional or accidental attack.

- On the Core Network, page 6-14 explains how an access control policy with strict rules can protect your critical assets.

- On a Remote or Mobile Network, page 6-15 explains how access control can monitor and protect the network from traffic at remote locations or on mobile devices.

Inside the Firewall

Managed devices inside the firewall monitor inbound traffic allowed by the firewall or traffic that passes the firewall due to misconfiguration. Common network segments include the DMZ, the internal network, the core, mobile access, and remote networks.

The diagram below illustrates traffic flow through the Firepower System, and provide some details on the types of inspection performed on that traffic. Note that the system does not inspect fast-pathed or blacklisted traffic. For traffic handled by an access control rule or default action, flow and inspection depend on the rule action. Although rule actions are not shown in the diagram for simplicity, the system does not perform any kind of inspection on trusted or blocked traffic. Additionally, file inspection is not supported with the default action.
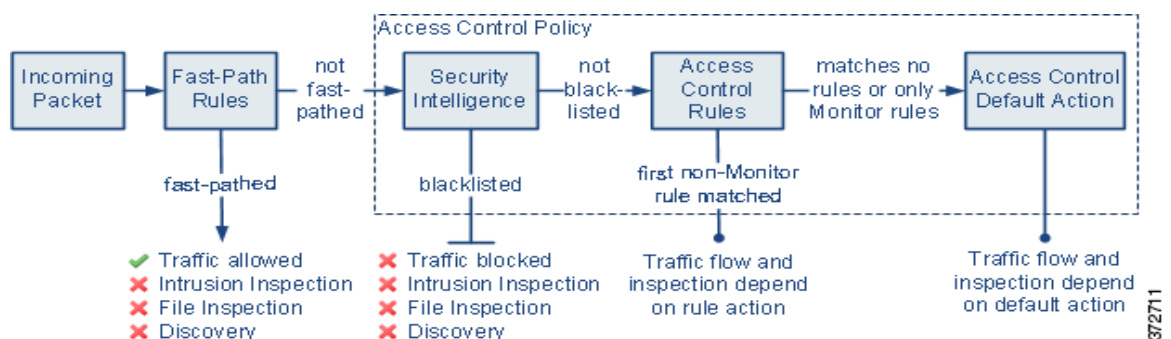
An incoming packet is first checked against any fast-path rules. If there is a match, the traffic is fast-pathed. If there is no match, Security Intelligence-based filtering determines if the packet is blacklisted. If not, any access control rules are applied. If the packet meets the conditions of a rule, traffic flow and inspection depend on the rule action. If no rules match the packet, traffic flow and inspection depend on the default policy action. (An exception occurs with Monitor rules, which allow traffic to continue to be evaluated.) The default action on each access control policy manages traffic that has not been fast-pathed or blacklisted, or matched by any non-Monitor rule. Note that fast-path is available only for 8000 Series devices.

You can create access control rules to provide more granular control over how you handle and log network traffic. For each rule, you specify an action (trust, monitor, block, or inspect) to apply to traffic that meets specific criteria.

On the DMZ

The DMZ contains outward-facing servers (for example, web, FTP, DNS, and mail), and may also provide services such as mail relay and web proxy to users on the internal network.

Content stored in the DMZ is static, and changes are planned and executed with clear communication and advance notice. Attacks in this segment are typically inbound and become immediately apparent because only planned changes should occur on the servers in the DMZ. An effective access control policy for this segment tightly controls access to services and searches for any new network events.

Servers in the DMZ can contain a database that the DMZ can query via the network. Like the DMZ, there should be no unexpected changes, but the database content is more sensitive and requires greater protection than a web site or other DMZ service. A strong intrusion policy, in addition to the DMZ access control policy, is an effective strategy.

A managed device deployed on this segment can detect attacks directed to the Internet that originate from a compromised server in the DMZ. Monitoring network traffic using Network Discovery can help you monitor these exposed servers for changes (for example, an unexpected service suddenly appearing) that could indicate a compromised server in the DMZ.
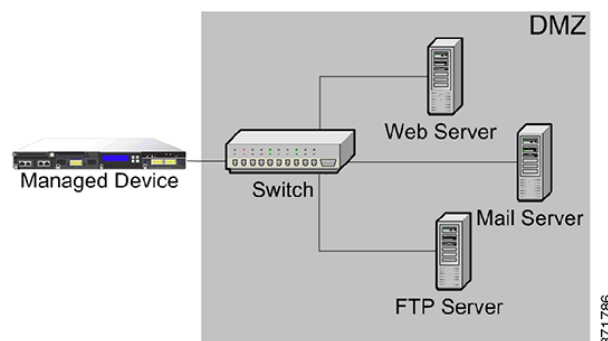
On the Internal Network

A malicious attack can originate from a computer on your internal network. This can be a deliberate act (for example, an unknown computer appears unexpectedly on your network), or an accidental infection (for example, a work laptop infected off-site is connected to the network and spreads a virus). Risk on the internal network can also be outbound (for example, a computer sends information to a suspicious external IP address).

This dynamic network requires a strict access control policy for all internal traffic in addition to outbound traffic. Add access control rules to tightly control traffic between users and applications.
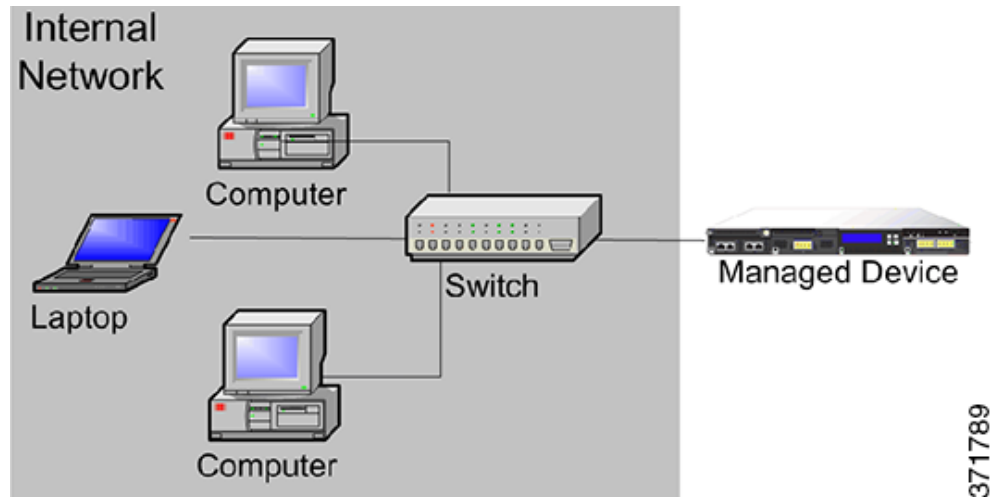
On the Core Network

Core assets are those assets critical to the success of your business that must be protected at all cost. Although core assets vary depending on the nature of your business, typical core assets include financial and management centers or intellectual property repositories. If the security on the core assets is breached, your business can be destroyed.

Although this segment must be readily available for your business to function, it must be tightly restricted controlled. Access control should ensure that these assets cannot be reached by those network segments with the highest risk, such as remote networks or mobile devices. Always use the most aggressive control on this segment, with strict rules for user and application access.
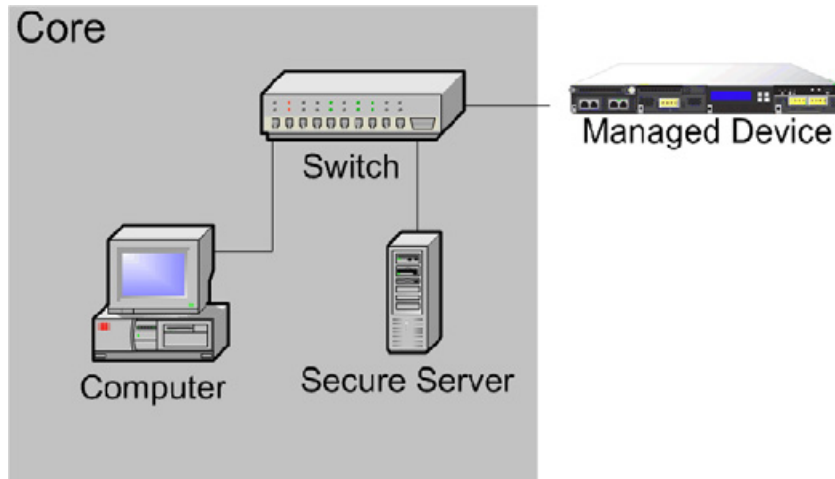
On a Remote or Mobile Network

Remote networks, located off-site, often use a virtual private network (VPN) to provide access to the primary network. Mobile devices and the use of personal devices for business purposes (for example, using a "smart phone" to access corporate email) are becoming increasingly common.

These networks can be highly dynamic environments with rapid and continual change. Deploying a managed device on a dedicated mobile or remote network allows you to create a strict access control policy to monitor and manage traffic to and from unknown external sources. Your policy can reduce your risk by rigidly limiting how users, network, and applications access core resources.
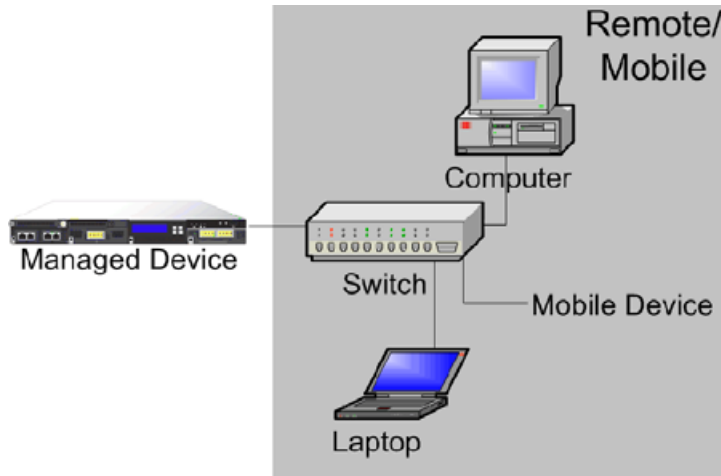
Using Multiple Sensing Interfaces on a Managed Device

The managed device offers multiple sensing interfaces on its network modules. You can use multiple sensing interfaces on managed devices to:

- recombine the separate connections from a network tap
- capture and evaluate traffic from different networks
- perform as a virtual router
- perform as a virtual switch

Note   Although each sensing interface is capable of receiving the full throughput for which the device is rated, the total traffic on the managed device cannot exceed its bandwidth rating without some packet loss.

Deploying multiple sensing interfaces on a managed device with a network tap is a straightforward process. The following diagram shows a network tap installed on a high-traffic network segment.
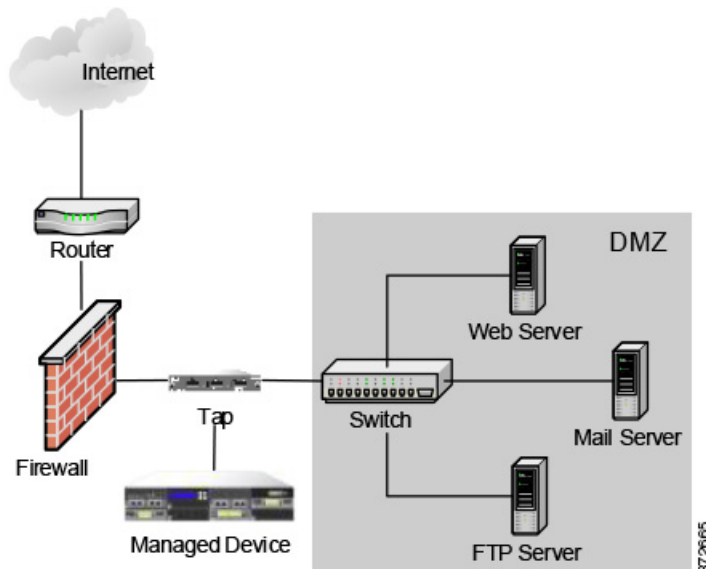

In this scenario, the tap transmits incoming and outgoing traffic through separate sensing interfaces. When you connect the multiple sensing interface adapter card on the managed device to the tap, the managed device is able to combine the traffic into a single data stream so that it can be analyzed.

Note that with a gigabit optical tap, as shown in the illustration below, both sets of sensing interfaces on the managed device are used by the connectors from the tap.
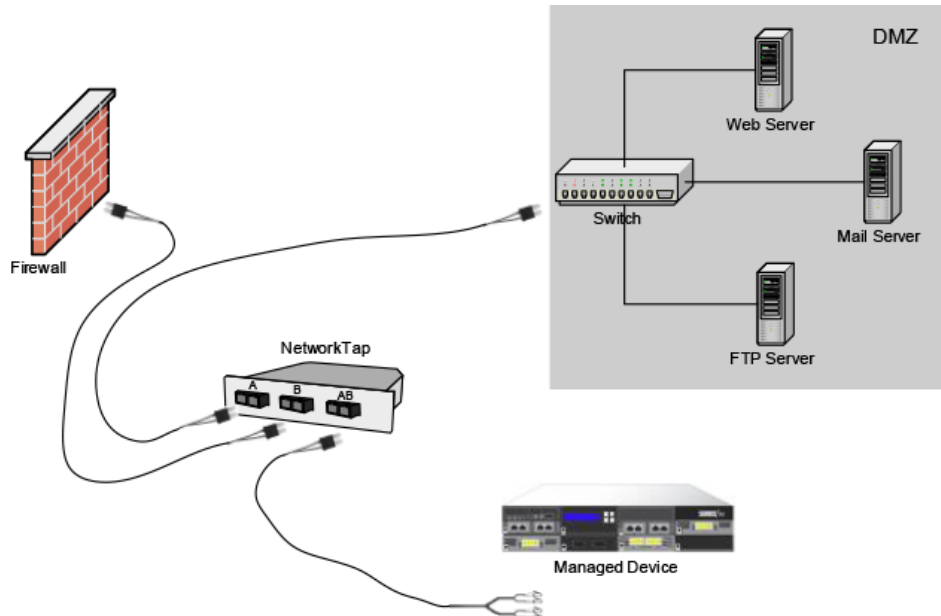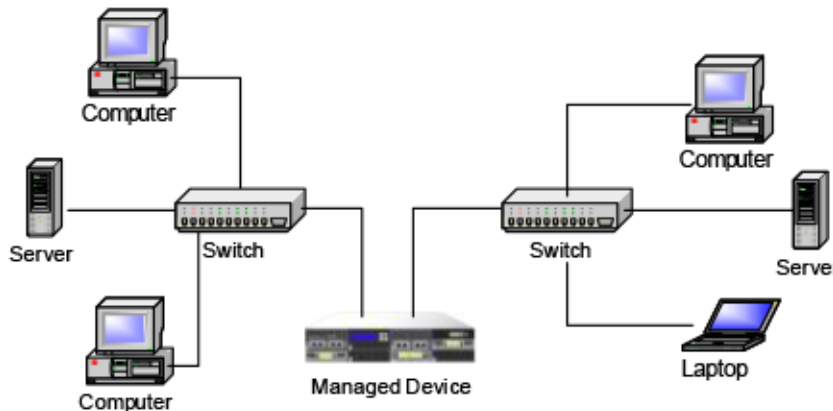
You can use the virtual switch to replace both the tap and the switch in your deployment. Note that if you replace the tap with a virtual switch, you lose the tap packet delivery guarantee.
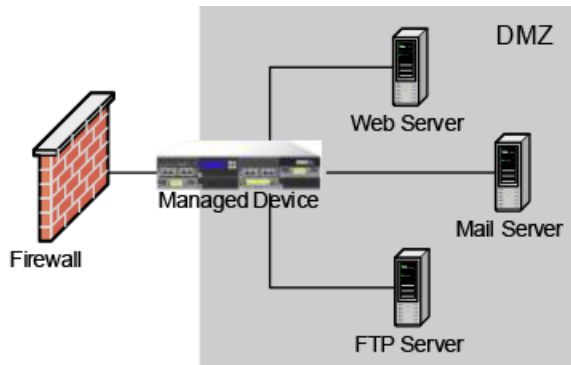

You can also create interfaces to capture data from separate networks. The following diagram shows a single device with a dual sensing interface adapter and two interfaces connected to two networks.

In addition to using one device to monitor both network segments, you can use the virtual switch capability of the device to replace both switches in your deployment.
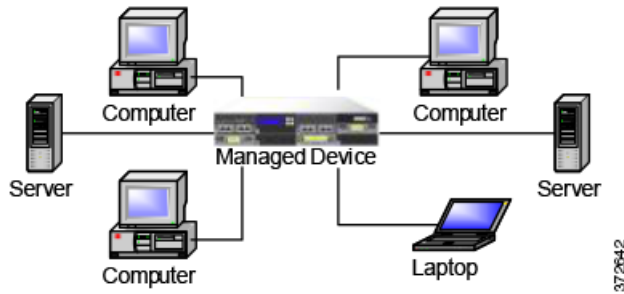
Complex Network Deployments

Your enterprise's network may require remote access, such as using a VPN, or have multiple entry points, such as a business partner or banking connection.

Integrating with VPNs

Virtual private networks, or VPNs, use IP tunneling techniques to provide the security of a local network to remote users over the Internet. In general, VPN solutions encrypt the data payload in an IP packet. The IP header is unencrypted so that the packet can be transmitted over public networks in much the same way as any other packet. When the packet arrives at its destination network, the payload is decrypted and the packet is directed to the proper host.

Because network appliances cannot analyze the encrypted payload of a VPN packet, placing managed devices outside the terminating endpoints of the VPN connections ensures that all packet information can be accessed. The following diagram illustrates how managed devices can be deployed in a VPN environment.
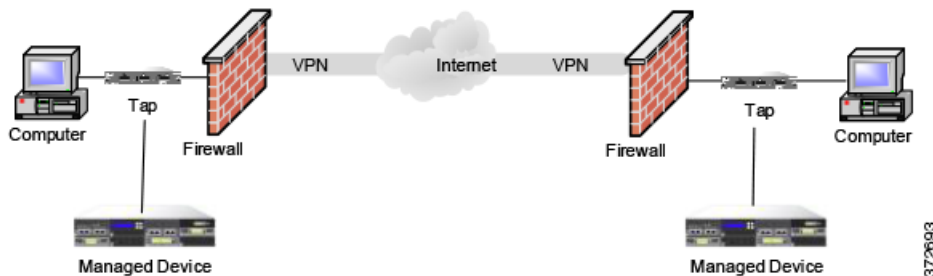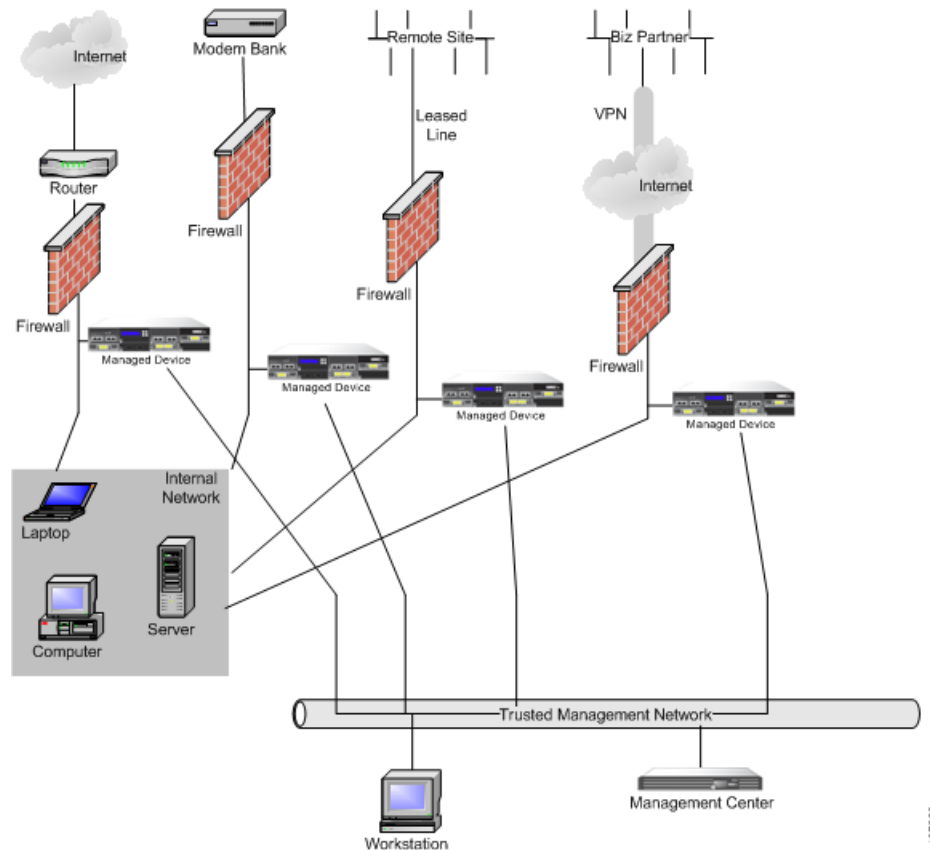

You can replace the firewall and the tap on either side of the VPN connection with the managed device. Note that if you replace the tap with a managed device, you lose the tap packet delivery guarantee.

Detecting Intrusions on Other Points of Entry

Many networks include more than one access point. Instead of a single border router that connects to the Internet, some enterprises use a combination of the Internet, modem banks, and direct links to business partner networks. In general, you should deploy managed devices near firewalls (either inside the firewall, outside the firewall, or both) and on network segments that are important to the integrity and confidentiality of your business data. The following diagram shows how managed devices can be installed at key locations on a complex network with multiple entry points.
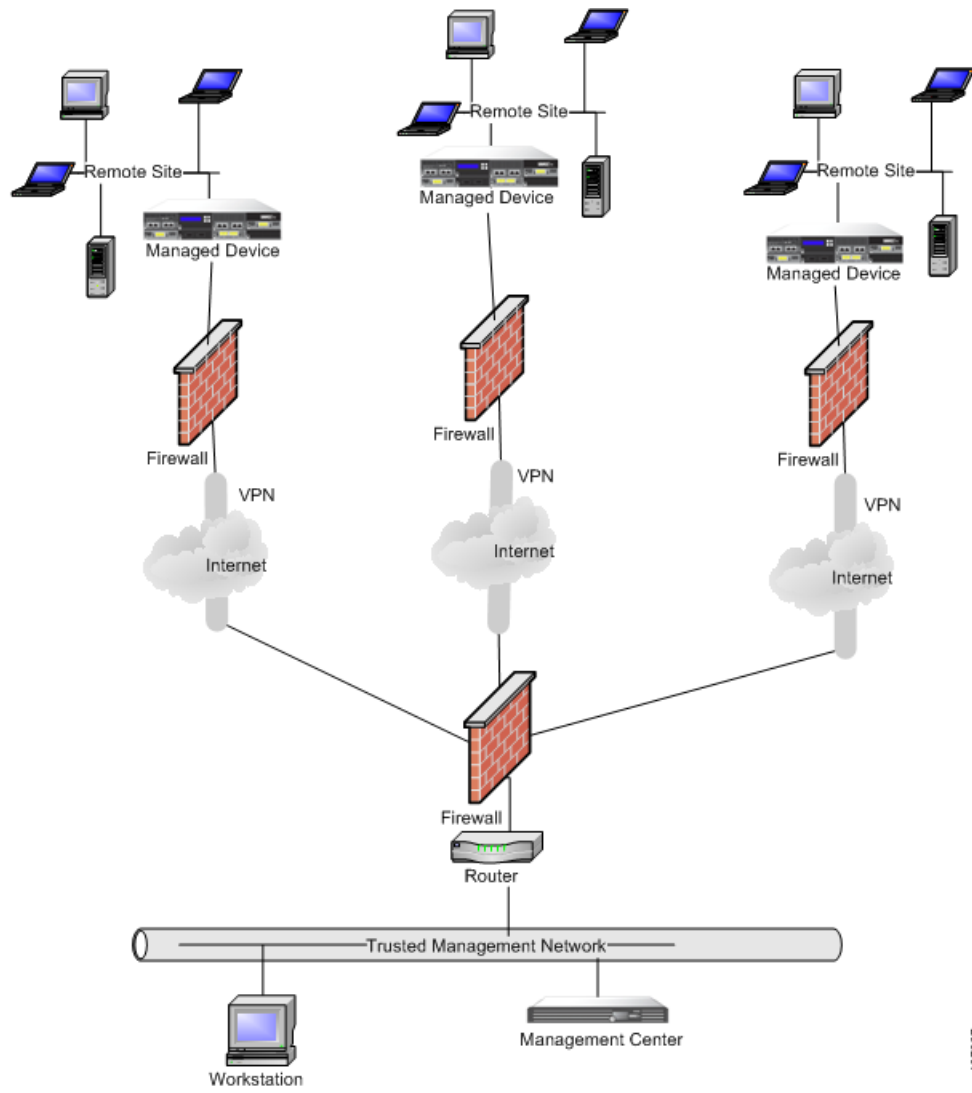

You can replace the firewall and the router with the managed device deployed on that network segment.
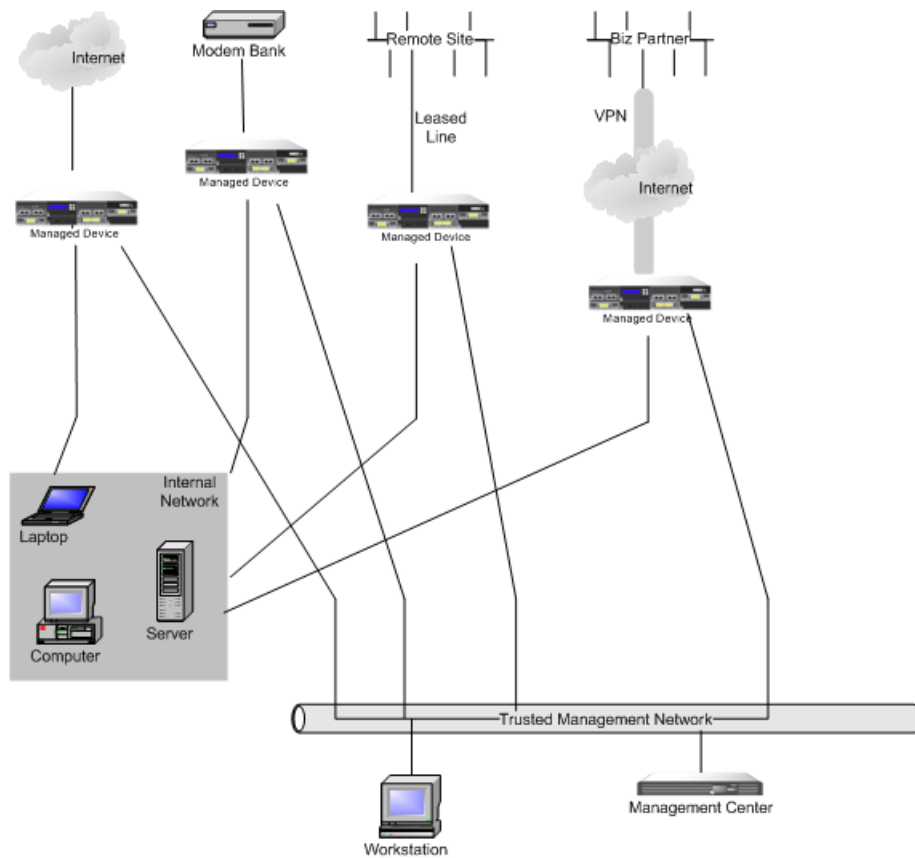
Deploying in Multi-Site Environments

Many organizations want to extend intrusion detection across a geographically disparate enterprise and then analyze all the data from one location. The Firepower System supports this by offering the Firepower Management Center, which aggregates and correlates events from managed devices deployed throughout the organization's many locations. Unlike deploying multiple managed devices and Firepower Management Centers in the same geographic location on the same network, when deploying managed devices in disparate geographic locations, you must take precautions to ensure the security of the managed devices and the data stream. To secure the data, you must isolate the managed devices and Firepower Management Center from unprotected networks. You can do this by transmitting the data stream from the managed devices over a VPN or with some other secure tunneling protocol as shown in the following diagram.

You can replace the firewalls and routers with the managed device deployed in each network segment.
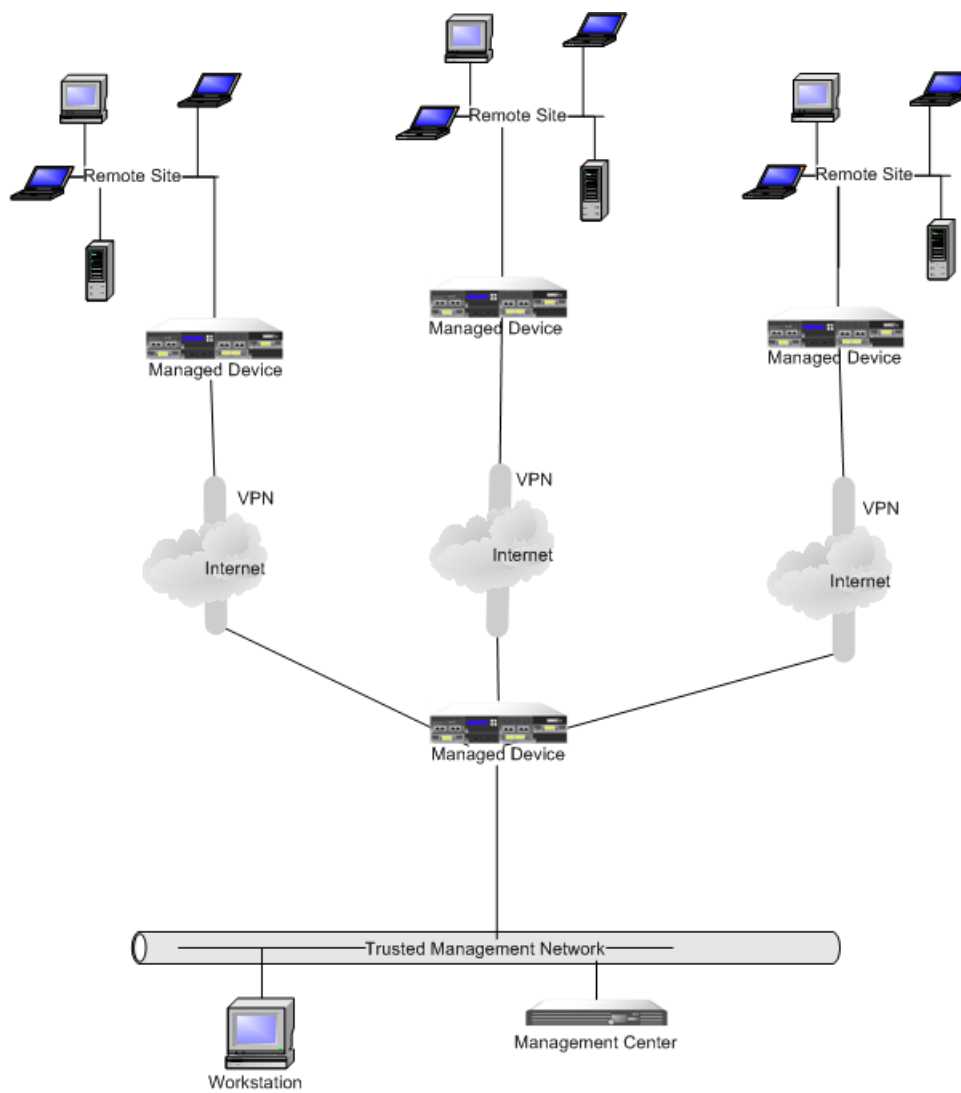
Integrating Multiple Management Interfaces within a Complex Network

You can configure multiple management interfaces in any deployment to isolate traffic from devices that monitor different networks and are managed by the same Firepower Management Center. Multiple management interfaces allow you to add a management interface with a unique IP address (IPv4 or IPv6) to your Firepower Management Center, and create a route from that management interface to a network that contains the device you want to manage. When you register your device to the new management interface, traffic on that device is isolated from traffic on devices registered to the default management interface on the Firepower Management Center.

Tip You must register a device to the static IP address of any management interface other than the default (eth0) management interface. DHCP is supported only on the default management interface.

Multiple management interfaces are supported in a NAT environment provided you do not use separate management interfaces for traffic channels. See Deploying on a Management Network, page 5-1 for more information. Note that Lights-Out Management is supported only on the default management interface, not additional management interfaces.

After you install your Firepower Management Center, you configure multiple management interfaces using the web interface. See Configuring Appliance Settings in the *Firepower Management Center Configuration Guide* for more information.

Integrating Managed Devices within Complex Networks

You can deploy managed devices in more complex network topologies than a simple multi-sector network. This section describes the issues surrounding network discovery and vulnerability analysis when deploying in environments where proxy servers, NAT devices, and VPNs exist, in addition to information about using the Firepower Management Center to manage multiple managed devices and the deployment and management of managed devices in a multi-site environment.

Integrating with Proxy Servers and NAT

Network address translation (NAT) devices or software may be employed across a firewall, effectively hiding the IP addresses of internal hosts behind a firewall. If managed devices are placed between these devices or software and the hosts being monitored, the system may incorrectly identify the hosts behind the proxy or NAT device. In this case, Cisco recommends that you position managed devices inside the network segment protected by the proxy or NAT device to ensure that hosts are correctly detected.

Integrating with Load Balancing Methods

In some network environments, "server farm" configurations are used to perform network load balancing for services such as web hosting, FTP storage sites, and so on. In load balancing environments, IP addresses are shared between two or more hosts with unique operating systems. In this case, the system detects the operating system changes and cannot deliver a static operating system identification with a high confidence value. Depending on the number of different operating systems on the affected hosts, the system may generate a large number of operating system change events or present a static operating system identification with a lower confidence value.

Other Detection Considerations

If an alteration has been made to the TCP/IP stack of the host being identified, the system may not be able to accurately identify the host operating system. In some cases, this is done to improve performance. For instance, administrators of Windows hosts running the Internet Information Services (IIS) Web Server are encouraged to increase the TCP window size to allow larger amounts of data to be received, thereby improving performance. In other instances, TCP/IP stack alteration may be used to obfuscate the true operating system to preclude accurate identification and avoid targeted attacks. The likely scenario that this intends to address is where an attacker conducts a reconnaissance scan of a network to identify hosts with a given operating system followed by a targeted attack of those hosts with an exploit specific to that operating system.

APPENDIX **A**

Power Requirements for Firepower 8000 Series Devices

Warnings and Cautions

This document contains both warnings and cautions. Warnings are safety related. Failure to follow warnings may lead to injury or equipment damage. Cautions are requirements for proper function. Failure to follow cautions may result in improper operation.

⚠️

Caution   The intra-building ports of the equipment or subassembly are suitable for connection to intra-building or exposed wiring or cabling only. The intra-building ports of the equipment or subassembly **must not** be metallically connected to interfaces that connect outside the plant (OSP) or its wiring. These interfaces are designed for use as intra-building interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE, Issue 4) and require isolation from the exposed OSP cabling. The addition of the primary protectors is not sufficient protection to connect these interfaces metallically to OSP wiring.

Static Control

⚠️

Caution   Electrostatic discharge control procedures, such as using grounded wrist straps and an ESD work surface, must be in place before unpacking, installing, or moving the appliance. Excessive electrostatic discharges can damage the appliance or cause unintended operation.

Firepower 81xx Family Appliances

This section describes the power requirements for:

- Firepower 8120, 8130, and 8140 (CHAS-1U-AC, CHAS-1U-DC, or CHAS-1U-AC/DC)

These appliances are suitable for installation by qualified personnel in network telecommunication facilities and locations where the National Electric Code applies.

Cisco recommends that you save the packing materials in case a return is necessary.

For more information, see the following sections:

- See AC Installation, page A-2 for circuit installation, voltage, current, and frequency range, and power cord information.

- See DC Installation, page A-3 for circuit installation, voltage, current, ground references, terminals, breaker requirements, and minimum wire size.
- See Grounding/Earthing Requirements, page A-4 for bonding locations, recommended terminals, ground wire requirements, and DC supplies.

AC Installation

The Firepower System must be installed in accordance with the requirements of Article 250 of NFPA 70, National Electric Code (NEC) Handbook, and local electrical codes.

⚠

Caution   Do **not** connect DC power to AC supplies.

Separate circuits are required to create redundant power sources. Use an uninterruptible or battery-backed power source to prevent power status issues or power loss due to input line power glitches.

Supply sufficient power to each power supply to run the entire appliance. The voltage and current ratings for each supply are listed on the label on the appliance.

Use an external Surge Protection Device at the input of the network equipment where the Firepower System is to be installed.

Separate Circuit Installation

If separate circuits are used, each one must be rated the full rating of the appliance. This configuration provides for circuit failure and power supply failure.

Example: Each supply is attached to a different 220V circuit. Each circuit must be capable of supplying 5A, as stated on the label.

Same Circuit Installation

If the same circuit is used to feed both supplies, then the power rating of one supply applies to the whole box. This configuration only provides protection from a power supply failure.

Example: Both supplies are attached to the same 220V circuit. The maximum draw from this circuit would be 5A, as stated on the label.

AC Voltage

The power supplies will work with these voltages: 100VAC to 240VAC nominal (85VAC to 264VAC maximum). Use of voltages outside this range may cause damage to the appliance.

AC Current

The labeled current rating for each supply is: 5.2A maximum over the full range, per supply 2.6A maximum for 187VAC to 264VAC, per supply. Appropriate wire and breakers must be used to reduce the potential for fire.

Frequency Range

The frequency range of the AC power supply is 47 Hz to 63 Hz. Frequencies outside this range may cause the appliance to not operate or to operate incorrectly.

Power Cords

The power connections on the power supplies are IEC C14 connectors and they will accept IEC C13 connectors. A UL-recognized power cord must be used. The minimum wire gauge is 16 AWG. The cords supplied with the appliances are 16 AWG, UL-recognized cords with NEMA 515P plug. Contact the factory about other power cords.

DC Installation

Separate circuits are required to create redundant power sources. Use an uninterruptible or battery-backed power source to prevent power status issues or power loss due to input line power glitches.

⚠
Caution   Do **not** connect AC power to DC supplies.

Supply sufficient power to each power supply to run the entire appliance. The voltage and current ratings for each supply are listed on the label on the appliance.

Use an external Surge Protection Device at the input of the network equipment where the Firepower System is to be installed.

Separate Circuit Installation

If separate circuits are used, each circuit must be rated to the full rating of the appliance. This configuration provides for circuit failure and power supply failure.

Example: Each supply is attached to a different –48VDC circuit. Each circuit must be capable of supplying 20A, as stated on the label.

Same Circuit Installation

If the same circuit is used to feed both supplies, then the power rating of one supply applies to the whole box. This configuration only provides protection from a power supply failure.

Example: Both supplies are attached to the same –48VDC circuit. The maximum draw from this circuit would be 20A, as stated on the label.

⚠
Caution   Use of this optimization requires that the power cords are rated for the full rating for each supply.

DC Voltage

The power supplies will work with these voltages:

- -48VDC nominal referenced to RTN

- -40VDC to -72VDC maximum

Use of voltages outside this range may cause damage to the appliance.

DC Current

11A maximum, per supply

Ground Reference

The DC power supplies are fully isolated from the ground reference.

Recommended Terminals

Power is connected to the DC supplies through screw terminals. Terminals must be UL approved. Terminals must have a hole supporting an M4 or a #8 screw. The maximum width of the terminal is 8.1mm (0.320"). A representative spade terminal for 10-12 gauge wire is Tyco 325197.

Breaker Requirements

A breaker sufficient to carry the rated current at the rated voltage must be provided. The circuit breaker must meet the following requirements:

- UL Recognized
- CSA Approved (Recommended)
- VDE Approved (Recommended)
- Support the maximum load (20A)
- Support the installation voltage (-40V to -72VDC, as required by the power supply)
- Rated for DC use

A recommended breaker is: Airpax IELK1-1-72-20.0-01-V. The terminal option used will depend on the installation. This breaker is a single pole, 20A breaker with a DC rating of 80V. It is listed as having a *long delay.* Information about this breaker can be found at http://www.airpax.net/site/utilities/eliterature/pdfs/ial.pdf.

Minimum Wire Size Requirements

Power feeds with three wires (one circuit) per raceway may use 12 AWG wire. Power feeds with more than one circuit per raceway must use 10 AWG wire. Note that the two separate feeds for the redundant supplies are two circuits and must use 10 AWG wire.
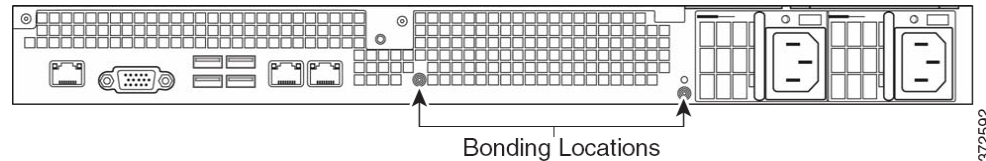
Grounding/Earthing Requirements

The Firepower System must be grounded to the Common Bonding Network.

Bonding Locations

Ground bonding locations are provided on the rear of the chassis. M4 studs are provided. Outside-toothed lock washers are provided for attaching ring terminals. A standard ground symbol is available by each stud.

The following illustration indicates the bonding locations on the 1U chassis.

Bonding Locations

Recommended Terminals

You must use UL-Approved terminals for the ground connection. Ring terminals with a clearance hole for 4mm or #8 studs may be used. For 10-12 AWG wire, Tyco 34853 is recommended. This is a UL-approved, ring terminal with a hole for a #8 stud.

Ground Wire Requirements

The ground wire must be sized sufficiently to handle the current of the circuit in case of a single fault. The size of the ground wire should be equal to the current of the breaker used to protect the circuit. For AC circuits, see AC Current, page A-2. For DC currents, see DC Current, page A-4.

Bare conductors must be coated with antioxidant before crimp connections are made. Only copper cables can be used for grounding purposes.

DC Supplies

The DC power supplies have additional ground connections on each supply. This allows the hot-swappable supply to be connected to power, return and ground so that it may be safely inserted. This ground lug must be attached.

It is a M4 screw with an outside-toothed lock washer screw.

The ground wire should be sized to match the breaker for the circuit.

Firepower 82xx Family Appliances

This section describes the power requirements for:

- Firepower 8250, 8260, 8270, and 8290 (CHAS-2U-AC, CHAS-2U-DC, or CHAS-2U-AC/DC)

These appliances are suitable for installation by qualified personnel in network telecommunication facilities and locations where the National Electric Code applies.

Cisco recommends that you save the packing materials in case a return is necessary.

For more information, see the following sections:

- See AC Installation, page A-6 for circuit installation, voltage, current, and frequency range, and power cord information.

- See DC Installation, page A-7 for circuit installation, voltage, current, ground references, terminals, breaker requirements, and minimum wire size.
- See Grounding/Earthing Requirements, page A-8 for bonding locations, recommended terminals, ground wire requirements, and DC supplies.

AC Installation

The Firepower System must be installed in accordance with the requirements of Article 250 of NFPA 70, National Electric Code (NEC) Handbook, and local electrical codes.

⚠️

Caution   Do **not** connect DC power to AC supplies.

Separate circuits are required to create redundant power sources. Use an uninterruptible or battery-backed power source to prevent power status issues or power loss due to input line power glitches.

Supply sufficient power to each power supply to run the entire appliance. The voltage and current ratings for each supply are listed on the label on the appliance.

Use an external Surge Protection Device at the input of the network equipment where the Firepower System is to be installed.

Separate Circuit Installation

If separate circuits are used, each one must be rated the full rating of the appliance. This configuration provides for circuit failure and power supply failure.

Example: Each supply is attached to a different 220V circuit. Each circuit must be capable of supplying 5A, as stated on the label.

Same Circuit Installation

If the same circuit is used to feed both supplies, then the power rating of one supply applies to the whole box. This configuration only provides protection from a power supply failure.

Example: Both supplies are attached to the same 220V circuit. The maximum draw from this circuit would be 5A, as stated on the label.

AC Voltage

The power supplies will work with these voltages: 100VAC to 240VAC nominal (85VAC to 264VAC maximum). Use of voltages outside this range may cause damage to the appliance.

AC Current

The labeled current rating for each supply is: 8A maximum over the full range, per supply 4A maximum for 187VAC to 264VAC, per supply. Appropriate wire and breakers must be used to reduce the potential for fire.

Frequency Range

The frequency range of the AC power supply is 47 Hz to 63 Hz. Frequencies outside this range may cause the appliance to not operate or to operate incorrectly.

Power Cords

The power connections on the power supplies are IEC C14 connectors and they will accept IEC C13 connectors. A UL-recognized power cord must be used. The minimum wire gauge is 16 AWG. The cords supplied with the appliances are 16 AWG, UL-recognized cords with NEMA 515P plug. Contact the factory about other power cords.

DC Installation

Separate circuits are required to create redundant power sources. Use an uninterruptible or battery-backed power source to prevent power status issues or power loss due to input line power glitches.

⚠
Caution   Do **not** connect AC power to DC supplies.

Supply sufficient power to each power supply to run the entire appliance. The voltage and current ratings for each supply are listed on the label on the appliance.

Use an external Surge Protection Device at the input of the network equipment where the Firepower System is to be installed.

Separate Circuit Installation

If separate circuits are used, each circuit must be rated to the full rating of the appliance. This configuration provides for circuit failure and power supply failure.

Example: Each supply is attached to a different –48VDC circuit. Each circuit must be capable of supplying 20A, as stated on the label.

Same Circuit Installation

If the same circuit is used to feed both supplies, then the power rating of one supply applies to the whole box. This configuration only provides protection from a power supply failure.

Example: Both supplies are attached to the same –48VDC circuit. The maximum draw from this circuit would be 20A, as stated on the label.

⚠
Caution   Use of this optimization requires that the power cords are rated for the full rating for each supply.

DC Voltage

The power supplies will work with these voltages:

- -48VDC nominal referenced to RTN

- -40VDC to -72VDC maximum

Use of voltages outside this range may cause damage to the appliance.

DC Current

18A maximum, per supply

Ground Reference

The DC power supplies are fully isolated from the ground reference.

Recommended Terminals

Power is connected to the DC supplies through screw terminals. Terminals must be UL approved. Terminals must have a hole supporting an M4 or a #8 screw. The maximum width of the terminal is 8.1mm (0.320"). A representative spade terminal for 10-12 gauge wire is Tyco 325197.

Breaker Requirements

A breaker sufficient to carry the rated current at the rated voltage must be provided. The circuit breaker must meet the following requirements:

- UL Recognized
- CSA Approved (Recommended)
- VDE Approved (Recommended)
- Support the maximum load (20A)
- Support the installation voltage (-40V to -72VDC, as required by the power supply)
- Rated for DC use

A recommended breaker is: Airpax IELK1-1-72-20.0-01-V. The terminal option used will depend on the installation. This breaker is a single pole, 20A breaker with a DC rating of 80V. It is listed as having a *long delay*. Information about this breaker can be found at http://www.airpax.net/site/utilities/eliterature/pdfs/ial.pdf.

Minimum Wire Size Requirements

Power feeds with three wires (one circuit) per raceway may use 12 AWG wire. Power feeds with more than one circuit per raceway must use 10 AWG wire. Note that the two separate feeds for the redundant supplies are two circuits and must use 10 AWG wire.
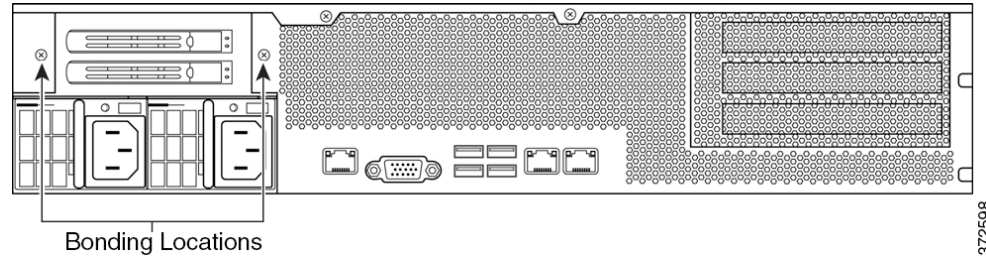
Grounding/Earthing Requirements

The Firepower System must be grounded to the Common Bonding Network.

Bonding Locations

Ground bonding locations are provided on the rear of the chassis. M4 studs are provided. Outside-toothed lock washers are provided for attaching ring terminals. A standard ground symbol is available by each stud.

The following illustration indicates the bonding locations on the 2U chassis.

Bonding Locations

Recommended Terminals

You must use UL-Approved terminals for the ground connection. Ring terminals with a clearance hole for 4mm or #8 studs may be used. For 10-12 AWG wire, Tyco 34853 is recommended. This is a UL-approved, ring terminal with a hole for a #8 stud.

Ground Wire Requirements

The ground wire must be sized sufficiently to handle the current of the circuit in case of a single fault. The size of the ground wire should be equal to the current of the breaker used to protect the circuit. For AC circuits, see AC Current, page A-2. For DC currents, see DC Current, page A-4.

Bare conductors must be coated with antioxidant before crimp connections are made. Only copper cables can be used for grounding purposes.

DC Supplies

The DC power supplies have additional ground connections on each supply. This allows the hot-swappable supply to be connected to power, return and ground so that it may be safely inserted. This ground lug must be attached.

It is a M4 screw with an outside-toothed lock washer screw.

The ground wire should be sized to match the breaker for the circuit.

Firepower and AMP 83xx Family Appliances

This section describes the power requirements for:

- Firepower and AMP 8350, 8360, 8370, and 8390 (PG35-2U-AC/DC)

These appliances are suitable for installation by qualified personnel in network telecommunication facilities and locations where the National Electric Code applies.

Cisco recommends that you save the packing materials in case a return is necessary.

For more information, see the following sections:

- See AC Installation, page A-10 for circuit installation, voltage, current, and frequency range, and power cord information.

- See DC Installation, page A-11 for circuit installation, voltage, current, ground references, terminals, breaker requirements, and minimum wire size.

- See Grounding/Earthing Requirements, page A-12 for bonding locations, recommended terminals, ground wire requirements, and DC supplies.

AC Installation

The Firepower System must be installed in accordance with the requirements of Article 250 of NFPA 70, National Electric Code (NEC) Handbook, and local electrical codes.

⚠

Caution   Do **not** connect DC power to AC supplies.

Separate circuits are required to create redundant power sources. Use an uninterruptible or battery-backed power source to prevent power status issues or power loss due to input line power glitches.

Supply sufficient power to each power supply to run the entire appliance. The voltage and current ratings for each supply are listed on the label on the appliance.

Use an external Surge Protection Device at the input of the network equipment where the Firepower System is to be installed.

Separate Circuit Installation

If separate circuits are used, each one must be rated the full rating of the appliance. This configuration provides for circuit failure and power supply failure.

Example: Each supply is attached to a different 220V circuit. Each circuit must be capable of supplying 10A, as stated on the label.

Same Circuit Installation

If the same circuit is used to feed both supplies, then the power rating of one supply applies to the whole box. This configuration only provides protection from a power supply failure.

Example: Both supplies are attached to the same 220V circuit. The maximum draw from this circuit would be 10A, as stated on the label.

AC Voltage

The power supplies will work with these voltages: 100VAC to 240VAC nominal (85VAC to 264VAC maximum). Use of voltages outside this range may cause damage to the appliance.

AC Current

The labeled current rating for each supply is: 11A maximum over the full range, per supply 5.5A maximum for 187VAC to 264VAC, per supply. Appropriate wire and breakers must be used to reduce the potential for fire.

Frequency Range

The frequency range of the AC power supply is 47 Hz to 63 Hz. Frequencies outside this range may cause the appliance to not operate or to operate incorrectly.

Power Cords

The power connections on the power supplies are IEC C14 connectors and they will accept IEC C13 connectors. A UL-recognized power cord must be used. The minimum wire gauge is 16 AWG. The cords supplied with the appliances are 16 AWG, UL-recognized cords with NEMA 515P plug. Contact the factory about other power cords.

DC Installation

Separate circuits are required to create redundant power sources. Use an uninterruptible or battery-backed power source to prevent power status issues or power loss due to input line power glitches.

⚠
Caution   Do **not** connect AC power to DC supplies.

Supply sufficient power to each power supply to run the entire appliance. The voltage and current ratings for each supply are listed on the label on the appliance.

Use an external Surge Protection Device at the input of the network equipment where the Firepower System is to be installed.

Separate Circuit Installation

If separate circuits are used, each circuit must be rated to the full rating of the appliance. This configuration provides for circuit failure and power supply failure.

Example: Each supply is attached to a different –48VDC circuit. Each circuit must be capable of supplying 25A, as stated on the label.

Same Circuit Installation

If the same circuit is used to feed both supplies, then the power rating of one supply applies to the whole box. This configuration only provides protection from a power supply failure.

Example: Both supplies are attached to the same –48VDC circuit. The maximum draw from this circuit would be 25A, as stated on the label.

⚠
Caution   Use of this optimization requires that the power cords are rated for the full rating for each supply.

DC Voltage

The power supplies will work with these voltages:

- -48VDC nominal referenced to RTN

        •   -40VDC to -72VDC maximum

Use of voltages outside this range may cause damage to the appliance.

DC Current

25A maximum, per supply

Ground Reference

The DC power supplies are fully isolated from the ground reference.

Recommended Terminals

Power is connected to the DC supplies through screw terminals. Terminals must be UL approved. Terminals must have a hole supporting an M4 or a #8 screw. The maximum width of the terminal is 8.1mm (0.320"). A representative spade terminal for 10-12 gauge wire is Tyco 325197.

Breaker Requirements

A breaker sufficient to carry the rated current at the rated voltage must be provided. The circuit breaker must meet the following requirements:

- UL Recognized
- CSA Approved (Recommended)
- VDE Approved (Recommended)
- Support the maximum load (20A)
- Support the installation voltage (-40V to -72VDC, as required by the power supply)
- Rated for DC use

A recommended breaker is: Airpax IELK1-1-72-20.0-01-V. The terminal option used will depend on the installation. This breaker is a single pole, 20A breaker with a DC rating of 80V. It is listed as having a *long delay*. Information about this breaker can be found at http://www.airpax.net/site/utilities/eliterature/pdfs/ial.pdf.

Minimum Wire Size Requirements

Power feeds with three wires (one circuit) per raceway may use 12 AWG wire. Power feeds with more than one circuit per raceway must use 10 AWG wire. Note that the two separate feeds for the redundant supplies are two circuits and must use 10 AWG wire.

Grounding/Earthing Requirements

The Firepower System must be grounded to the Common Bonding Network.

Bonding Locations

Ground bonding locations are provided on the rear of the chassis. M4 studs are provided. Outside-toothed lock washers are provided for attaching ring terminals. A standard ground symbol is available by each stud.

The following illustration indicates the bonding locations on the 83xx Family 2U chassis.
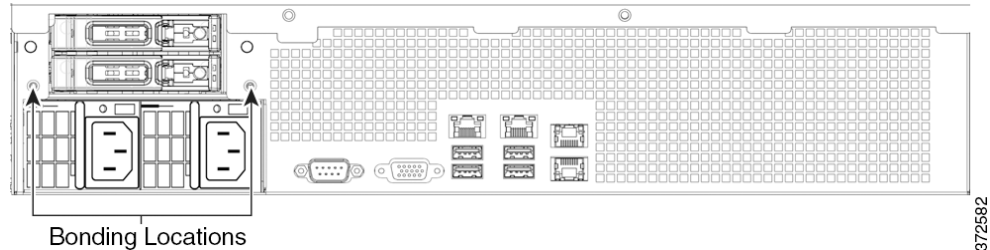
Bonding Locations

Recommended Terminals

You must use UL-Approved terminals for the ground connection. Ring terminals with a clearance hole for 4mm or #8 studs may be used. For 10-12 AWG wire, Tyco 34853 is recommended. This is a UL-approved, ring terminal with a hole for a #8 stud.

Ground Wire Requirements

The ground wire must be sized sufficiently to handle the current of the circuit in case of a single fault. The size of the ground wire should be equal to the current of the breaker used to protect the circuit. For AC circuits, see AC Current, page A-10. For DC currents, see DC Current, page A-12.

Bare conductors must be coated with antioxidant before crimp connections are made. Only copper cables can be used for grounding purposes.

DC Supplies

The DC power supplies have additional ground connections on each supply. This allows the hot-swappable supply to be connected to power, return and ground so that it may be safely inserted. This ground lug must be attached.

It is a M4 screw with an outside-toothed lock washer screw.

The ground wire should be sized to match the breaker for the circuit.

APPENDIX **B**

Inserting and Removing Firepower 8000 Series Network Modules

The Firepower 8000 Series devices use network modules (NetMods) that contain either copper or fiber sensing interfaces, allowing for modular flexibility in your deployment. The devices can be shipped fully assembled or you can install the modules. You may also need to replace or change a module.

Use the procedures in this section to insert a new NetMod or to remove or replace a preinstalled NetMod.

⚠️

Caution   You **cannot** hot-swap NetMods. You must power down and unplug **both** power cords from the appliance before inserting or removing modules.

✎

Note   When replacing NetMods on a stacked configuration, complete all procedures on the secondary units first, then perform any replacements on the primary unit.

About Firepower 8000 Series Modules

For a new appliance, assemble your device before installing the Firepower System. See the assembly instructions included with your NetMods.

✎

Note   Replacing a NetMod can alter the configuration of a fully configured Korean-certified (KCC mark) Firepower device. For more information, see the original configuration documentation for your appliance and the *Regulatory Compliance and Safety Information for FirePOWER and FireSIGHT Appliances* document.

Identify the Module Parts

The sensing interfaces for the Firepower 8000 Series appliances can be delivered with copper or fiber interfaces, and can have configurable bypass sensing interfaces or non-bypass sensing interfaces. All NetMods contain the same parts, regardless of sensing interface, speed, or size of the module.
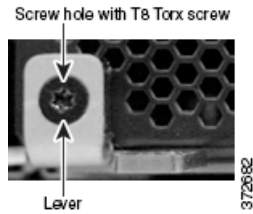
Figure B-1   Example NetMod or Slot Cover (open)
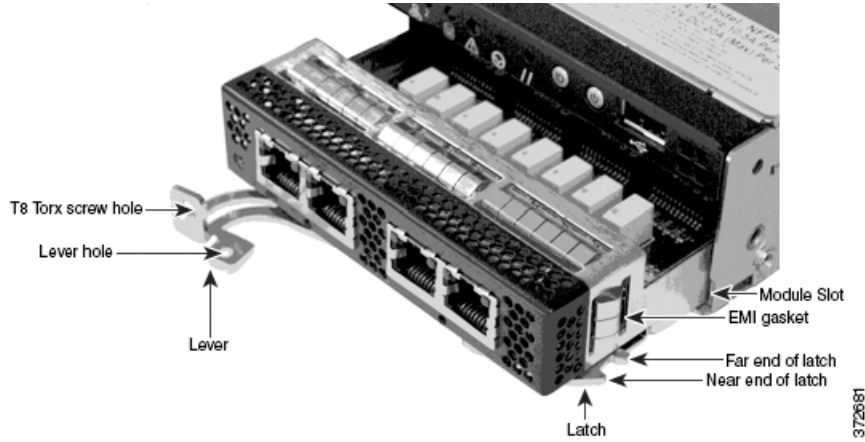
*Figure B-2   Example NetMod Lever (closed with screw in hole)*

See Firepower 8000 Series Modules, page 2-13 for complete information about Firepower 8000 Series modules.

Module Slots on the Firepower 8000 Series Devices

The following illustrations of the front of the chassis indicates the location of the module slots that contain NetMods for sensing interfaces.

- Firepower 81xx Family devices can use the modules in the following slots:

Figure B-3   Firepower 81xx Family Primary Device
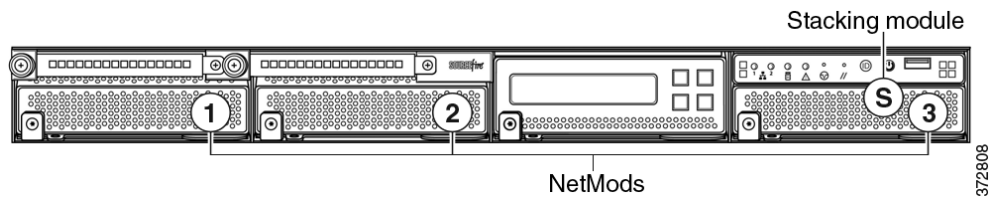
- Firepower 82xx Family and 83xx Family devices can use the modules in the following slots:

Figure B-4   Firepower 82xx Family and 83xx Family Primary Device
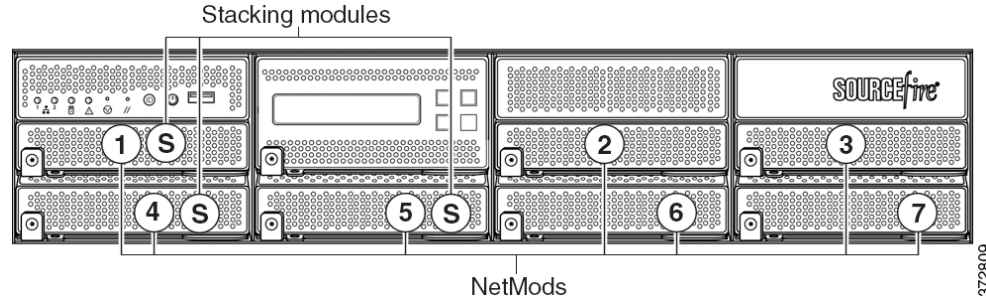
Stacking Configuration Considerations

A stacking module combines the resources of two or more identically configured appliances. See Firepower 8000 Series Stacking Module, page 3-9 for information about which Firepower 8000 Series models support stacking. Configure the modules as follows for stacked devices:

- You can use a device stack as you would a single device in your deployment, with a few exceptions. If you have Firepower 8000 Series devices in a high-availability pair, you cannot stack a device high-availability pair or a device in a high-availability pair.

- When replacing NetMods on a stacked configuration, complete all procedures on the secondary units first, then perform any replacements on the primary unit.

- Install NetMods on the primary device only.

- Install one stacking module on the primary device for each stacked secondary device, and one stacking module on each secondary device.

See Using Devices in a Stacked Configuration, page 3-10 for complete information about stacking. See the "8000 Series Device Stacking" chapter in the *Firepower Management Center Configuration Guide* for information about managing device stacks with your Firepower Management Center.

Included Items

Your module assembly kit includes a T8 Torx screwdriver and one or more of the following modules:

- quad-port 1000BASE-T copper configurable bypass NetMod. For more information, see Quad-Port 1000BASE-T Copper Configurable Bypass NetMod, page 2-13.

- quad-port 1000BASE-SX fiber configurable bypass NetMod. For more information, see Quad-Port 1000BASE-SX Fiber Configurable Bypass NetMod, page 2-14.

- dual-port 10GBASE (MMSR or SMLR) fiber configurable bypass NetMod. For more information, see Dual-Port 10GBASE (MMSR or SMLR) Fiber Configurable Bypass NetMod, page 2-16.

- dual-port 40GBASE-SR4 fiber configurable bypass NetMod. For more information, see Dual-Port 40GBASE-SR4 Fiber Configurable Bypass NetMod, page 2-17.

Note   Use this dual-slot NetMod only on the 40G-capacity Firepower 8250 or Firepower or AMP 8350. If you need to upgrade your device, see the *Cisco 8000 Series Device 40G Capacity Upgrade Guide*.

- quad-port 1000BASE-T copper non-bypass NetMod. For more information, see Quad-Port 1000BASE-T Copper Non-Bypass NetMod, page 2-19.

- quad-port 1000BASE-SX fiber non-bypass NetMod.quad-port 1000BASE-SX fiber non-bypass NetMod. For more information, see Quad-Port 1000BASE-SX Fiber Non-Bypass NetMod, page 2-19.

- quad-port 10GBASE (MMSR or SMLR) fiber non-bypass NetMod. For more information, see Quad-Port 10GBASE (MMSR or SMLR) Fiber Non-Bypass NetMod, page 2-20.

⚠

Caution   The quad-port 10GBASE fiber non-bypass NetMod contains non-removable small form factor pluggable (SFP) transceivers. Any attempt to remove the SFPs can damage the module.

- stacking module. For more information, see Stacking Module, page 2-21.

✎

Note   If you install a NetMod in an incompatible slot on your Firepower device or a NetMod is otherwise incompatible with your system, an error or warning message appears in the web interface on the managing Management Center when you attempt to configure the NetMod. Contact support for assistance.

Power Down the Appliance

⚠

Caution   You **cannot** hot-swap NetMods. You must power down and unplug **both** power cords from the appliance before inserting or removing modules.

Before You Begin

Prepare to insert or remove your module using the following guidelines:

- Identify all appliance and module parts.
- Identify the slots where you want to install your NetMods.

🔍

Tip   You can insert the NetMod into any available, compatible slot.

- Confirm that the EMI gaskets are in place.
- If your appliance is part of a device stack or high-availability pair, place the device in maintenance mode from the Firepower Management Center:
  - Choose **Devices > Device Management**.
  - Next to the stack member or peer you want to place into maintenance mode, click the toggle maintenance mode icon (🔧).
  - Click **Yes** to confirm maintenance mode.

Procedure

Step 1   To shut down the appliance, choose **System > Configuration**.

Step 2   Choose **Process**.

Step 3   Click **Run Command** next to **Shutdown Appliance**.

Step 4   Unplug all power cords from the appliance.

.

Related Topics

- "Placing a High-Availability Peer into Maintenance Mode" chapter in the *Firepower Management Center Configuration Guide*.

- "Replacing a Device in a Stack in a High-Availability Pair" chapter in the *Firepower Management Center Configuration Guide*.
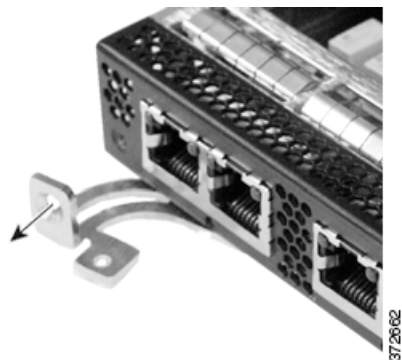
Remove the Module or Slot Cover

Use proper electrostatic discharge (ESD) practices such as wearing wrist straps and using an ESD work surface when handling the modules. Store unused modules in an ESD bag or box to prevent damage.

Procedure

Step 1   Remove and reserve the T8 Torx screw from the lever of the module using the included screwdriver.
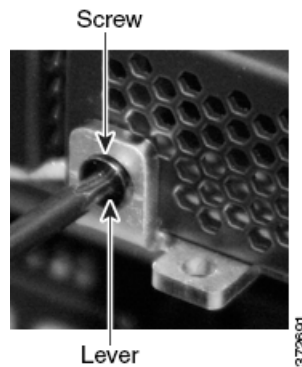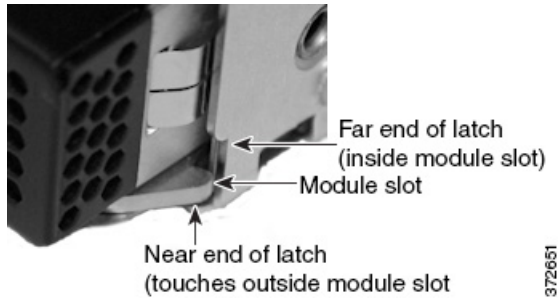

Step 2   Pull the lever away from the module to release the latch.

Step 3   Slide the module out of the slot.
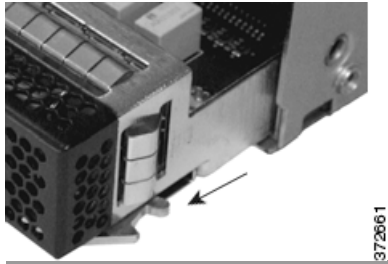
Insert the Module or Slot Cover

Use proper electrostatic discharge (ESD) practices such as wearing wrist straps and using an ESD work surface when handling the modules. Store unused modules in an ESD bag or box to prevent damage.

Procedure

Step 1   Remove and reserve the T8 Torx screw from the lever of the module using the included screwdriver.
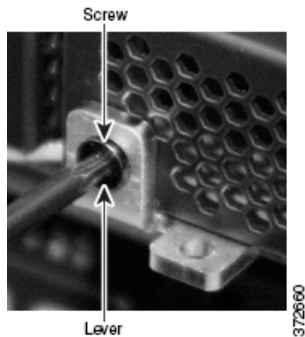
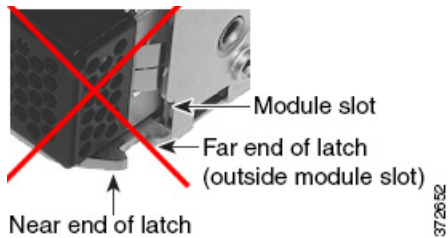Step 2   Pull the lever away from the module to open the latch. The near end of the latch is visible. The far end of the latch is inside the module.

Far end of latch
(engaged inside
module slot)

Near end of latch
(engaged outside module slot)

372653
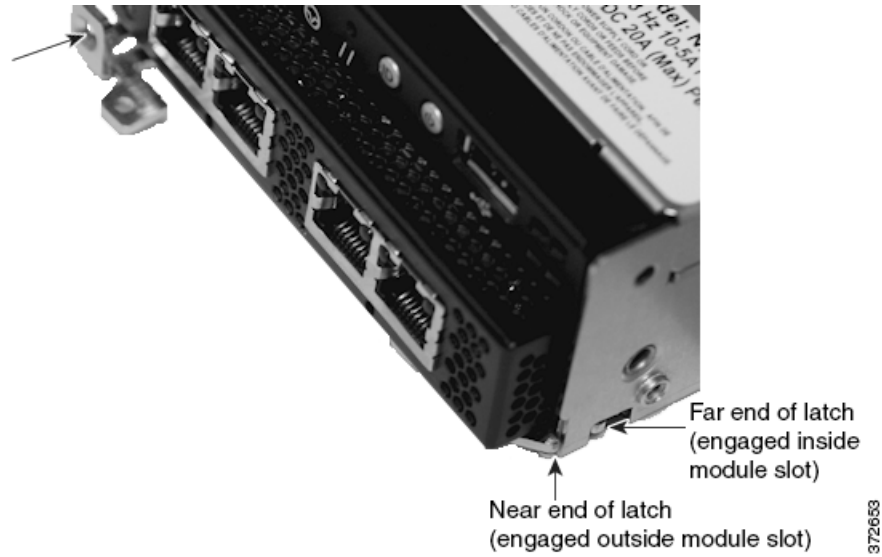
Step 3   Insert the module into the slot until the far end of the latch is inside the slot and the near end of the latch touches the outside of the module slot.

Correct module alignment

Far end of latch
(inside module slot)
Module slot

Near end of latch
(touches outside module slot

372651

Incorrect module alignment

Module slot
Far end of latch
(outside module slot)

Near end of latch

372652

Step 4   Push the lever toward the module so that the latch engages and pulls the module into the slot.

Far end of latch
(engaged inside
module slot)

Near end of latch
(engaged outside module slot)

⚠
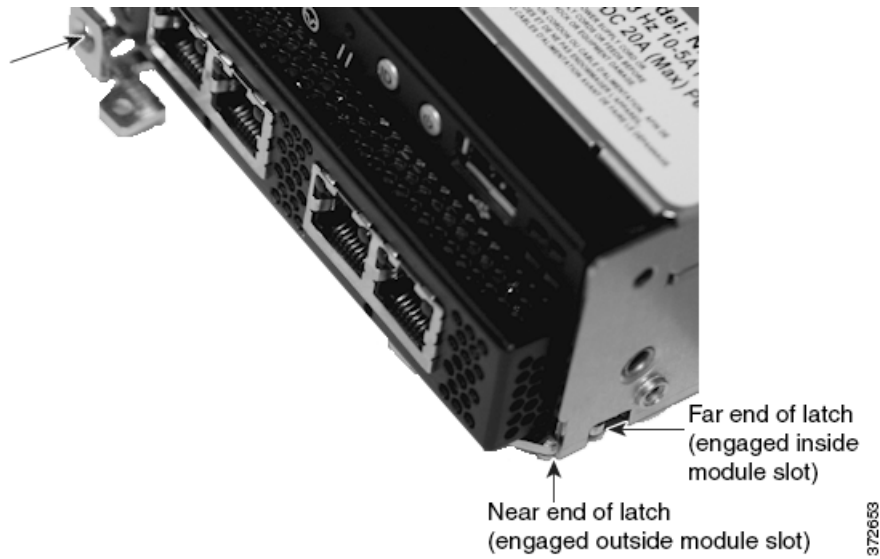
Caution   Do **not** use excessive force. If the latch does not engage, remove and realign the module, then try again.

Step 5   Press firmly on the screw hole to push the lever fully against the module to secure the latch.

The lever is fully against the module, and the module is flush with the chassis.
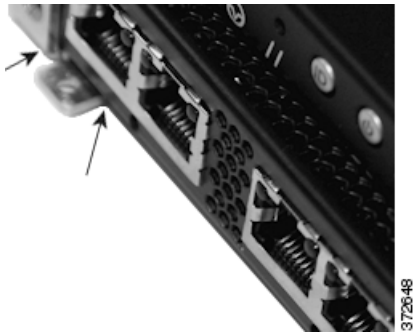
Step 6   Insert and tighten the reserved T8 Torx screw into the lever.

Screw

Lever
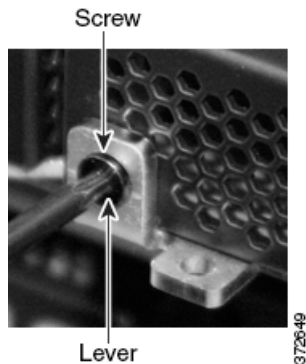
Restart the Appliance

Before You Begin

- Plug in all power cords to the appliance.

- Wait until the appliance is fully powered up. This could take several minutes.

Procedure

Step 1   Choose **System > Configuration**.

Step 2   Choose **Process**.

Step 3   Click **Run Command** next to **Restart Appliance Console**.

Verify the NetMod from the Firepower Management Center

Procedure

Step 1   Choose **Devices > Device Management**.

Step 2   Next to the device where you want to view the interfaces, click the edit icon ( ).

Step 3   Verify the interfaces on the **Interfaces** tab.

Step 4   If your appliance is part of a device stack or high-availability pair, bring the device out of maintenance mode from the Firepower Management Center:

- Choose **Devices > Device Management**.

- Next to the stack member or peer, click the toggle maintenance mode icon ( ) to bring the device out of maintenance mode.

What to Do Next

- Configure the new interfaces. See the "Interface Configuration Settings" chapter in the *Firepower Management Center Configuration Guide*.

- Apply the configuration changes.

Apply Changes to the Appliance

After you make changes to the configuration of a device, a device cluster, or a device stack, you must apply the changes before they take effect throughout the system. Note that the device must have unapplied changes or this option remains disabled.

Note that if you edit interfaces and reapply a device policy, Snort restarts for all interface instances on the device, not just those that you edited.

Tip   You can apply device changes from the Device Management page or from the **Interfaces** tab of the appliance editor.

Procedure

Step 1   Select **Devices > Device Management**.

Step 2   Next to the device where you want to apply changes, click the apply icon ( ).

Step 3   When prompted, click **Apply**.

Installing a Malware Storage Pack

You can install a malware storage pack in Firepower 8000 Series devices. A malware storage pack is an optional second solid-state drive (SSD) for expanded local file storage of suspected malware.

A malware storage pack kit, available from Cisco, contains everything you need to install a malware storage pack in your device. Each kit includes a malware storage pack mounted in a chassis-compatible SSD tray and an installation tool. You remove the empty second SSD tray and replace it with the compatible malware storage pack.

⚠

Caution Do not attempt to install a hard drive that was not supplied by Cisco in your device. Installing an unsupported hard drive may damage the device. Malware storage pack kits are available for purchase **only** from Cisco, and are for use **only** with version 5.3 or greater of the Firepower System. Contact Cisco Support if you require assistance with malware storage packs.

These instructions are for use with Firepower 8000 Series devices running version 5.3 or greater of the Firepower System, and contains the following sections:

Malware Storage Pack Overview

Firepower 8000 Series devices ship with a solid-state drive (SSD) that functions as the primary system drive used for the operating system, the Firepower System software, and local file storage of events and configuration files. As part of the *advanced malware protection* feature, you can configure the Firepower System to detect, store, track, analyze, and optionally block malware files being transmitted on your network. On detection, the *file storage* feature allows a device to store an eligible file to the hard drive.

When you configure a device to store files, it allocates a set portion of the primary hard drive's space solely to captured file storage. Based on your file policy configuration, your device may store a substantial amount of files to the hard drive.

The malware storage pack provides expanded local file storage of suspected malware and is available as an optional feature on the 8000 Series devices. When you install a malware storage pack in a device and configure the device to store files, the device allocates the entire malware storage pack for storing captured files, allowing more room on the primary hard drive to store events and configuration files.

Note   Certain aspects of advanced malware protection and file control require that you enable specific licensed capabilities on target devices. See the *Firepower Management Center Configuration Guide* for more information.

This document explains the following concepts and procedures:

- which devices support a malware storage pack
- what you need to install a malware storage pack
- how to install a malware storage pack in specific device types
- how to resume normal operations after you install a malware storage pack

Supported Devices

You can install a malware storage pack in 8000 Series devices running version 5.3 or greater of the Firepower System. The following 8000 Series devices support the malware storage pack:

- 81xx Family devices (Firepower 8120, 8130, 8140, but **not** the AMP8150)
- 82xx Family devices (Firepower 8250, 8260, 8270, 8290)
- 83xx Family devices (Firepower 8350, 8360, 8370, 8390)

You must be running version 5.3 or greater of the Firepower System software before you install the malware storage pack. For additional guidance, contact Cisco Support.

Caution   Before you update any part of the Firepower System, you must read the release notes or advisory text that accompanies the update. The release notes provide important information, including supported platforms, compatibility, prerequisites, warnings, and specific installation and uninstallation instructions.

Before You Begin

Before you install a malware storage pack in a Firepower 8000 Series device, take a moment to examine the contents of your malware storage pack installation kit and the device where the malware storage pack will be installed. Your malware storage pack installation kit contains the following items:

- a malware storage pack mounted in a chassis-compatible SSD tray
- an installation tool
- an instruction guide (this document)

There are two types of installation kits. The 1U chassis kit fits the 81xx Family of devices, and the 2U chassis kit fits both the 82xx Family and 83xx Family of devices.

Examine both your kit and your device to ensure that you have the appropriate malware storage pack kit for your device. Contact Cisco Support if you have any questions or concerns about your kit. See the following sections for more information:

- Malware Storage Pack Kit for 1U Devices, page C-3
- Malware Storage Pack Kit for 2U Devices, page C-3

Malware Storage Pack Kit for 1U Devices

The 81xx Family of devices requires a malware storage pack kit for the 1U chassis consisting of:

- a malware storage pack installed in a chassis-compatible SSD tray
- a T8 Torx driver
- an instruction guide (this document)
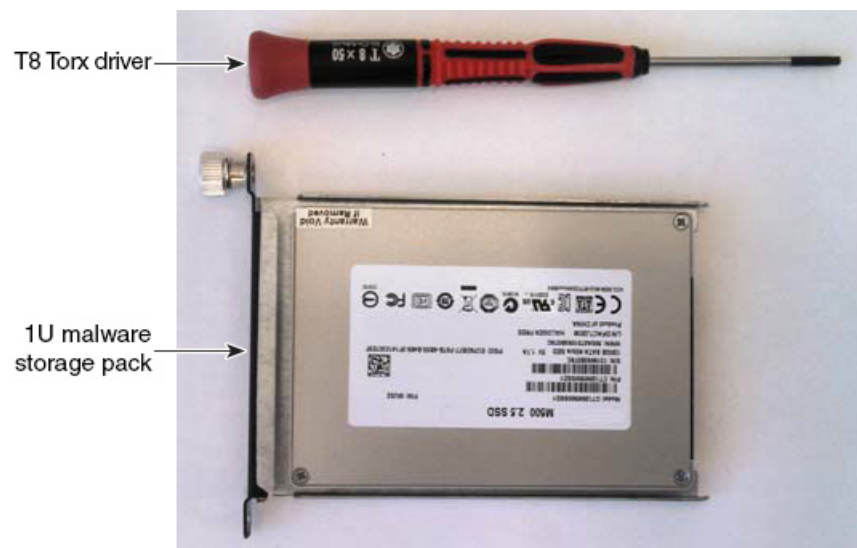
Malware Storage Pack Kit for 2U Devices

The 82xx Family and 83xx Family of devices require a malware storage pack kit for the 2U chassis consisting of:

- a malware storage pack installed in a chassis-compatible SSD tray
- a 3mm hex wrench

Installation

You can install a malware storage pack to an 8000 Series device already deployed in the field. Use these instructions to handle the following scenarios:

- installing a malware storage pack during a customer upgrade, where you install the malware storage pack and reimage the Firepower System

- installing a malware storage pack after a customer upgrade, where you reimage the Firepower System first, and then install the malware storage pack

Note   For information on how to safely shut down or restart the device, see the Managing Devices chapter in the *Firepower Management Center Configuration Guide.*

Installing a Malware Storage Pack During an Upgrade

Use the following procedure to install a malware storage pack in a device in the field and reimage the Firepower System.

To install a malware storage pack during a customer upgrade:

Step 1   Shut down the system.

Step 2   Power off the device.

Step 3   Install the malware storage pack:

- For 81xx Family devices, refer to <Blue>Instructions for the 81xx Family Devices on page 5.

- For 82xx Family and 83xx Family devices, refer to <Blue>Instructions for the 82xx Family and 83xx Family Devices on page 8.

Step 4   Reimage the device. Follow the instructions in the *Cisco Firepower 8000 Series Getting Started Guide* and the release notes or advisory text that accompanies the software update.

Step 5   Turn on the system.

Refer to <Blue>Post Installation on page 11 for information on restarting a device after a malware storage pack has been installed.

Installing a Malware Storage Pack on a Version 6.0.1 Device

Use the following procedure to install a malware storage pack in a device already configured and running Firepower System version 5.3 or greater.

To install malware storage pack in a device running version 5.3 or greater:

Step 1   Shut down the system.

Step 2   Power off the device.

Step 3   Install the malware storage pack:

- For 81xx Family devices, refer to <Blue>Instructions for the 81xx Family Devices on page 5.
- For 82xx Family and 83xx Family devices, refer to <Blue>Instructions for the 82xx Family and 83xx Family Devices on page 8.

Step 4   Turn on the system.

- Refer to <Blue>Post Installation on page 11 for information on restarting a device after a second SSD has been installed.

Instructions for the 81xx Family Devices

The following section describes how to install a malware storage pack in the 81xx Family of devices, which includes the Firepower 8120, 8130, and 8140 devices. Note that the malware storage pack is **not** supported on the AMP8150 device.

81xx Family Chassis Front View

The SSD trays are located on the front of the 81xx Family chassis.

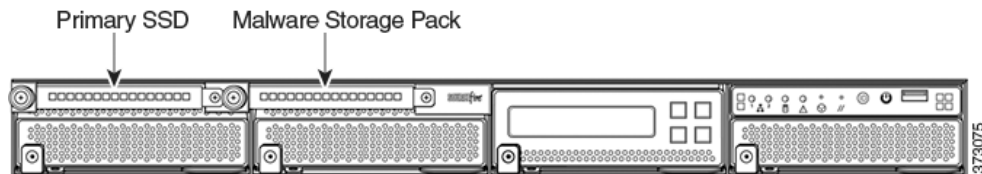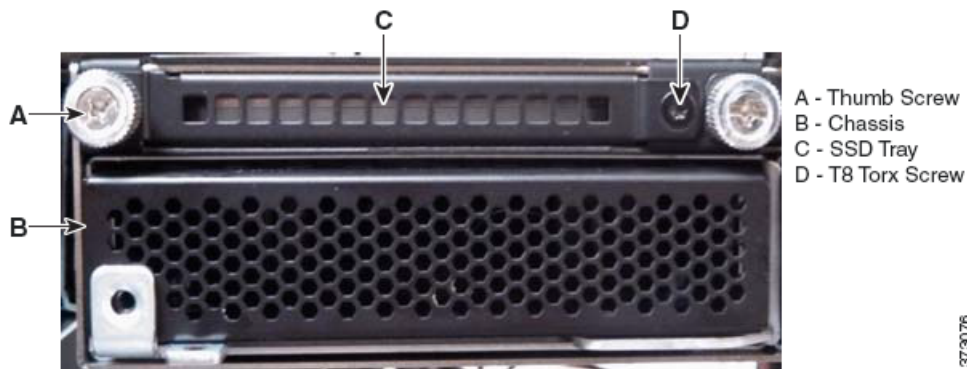*Figure C-1   81xx Family (Chassis: CHAS-1U-AC/DC) Front View*

Figure C-2   SSD Detail

The following steps describe how to install a malware storage pack in the 81xx Family of devices. Install the malware storage pack in the SSD bay labeled *Malware Storage Pack*. Remove the empty SSD tray and replace it with the appropriate malware storage pack.

Note   Use proper electrostatic discharge (ESD) practices such as wrist straps and an ESD work surface.

Step 1   Ensure the device is powered off before you begin to install or remove a malware storage pack.

Step 2   Use the T8 Torx driver to remove the Torx screw on the right side of the second SSD tray. Retain the screw.

Step 3   Unscrew and pull on the thumbscrew to remove the empty SSD tray from the device.

Note   Retain the empty SSD tray. If you need to remove the malware storage pack at any time, reinstall the empty tray in the device.
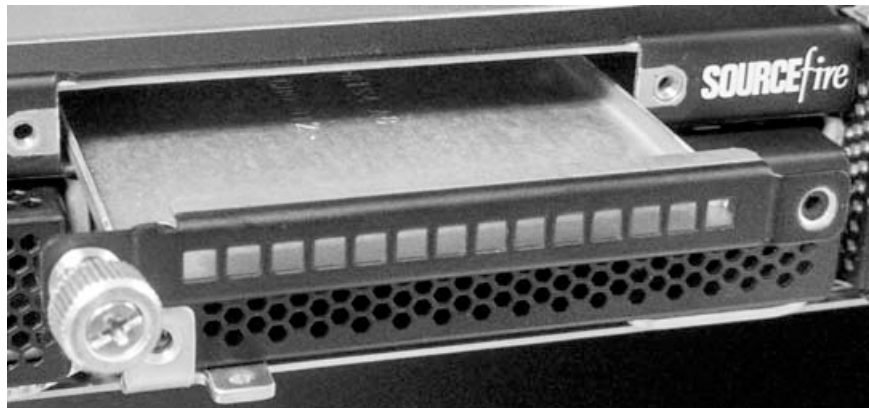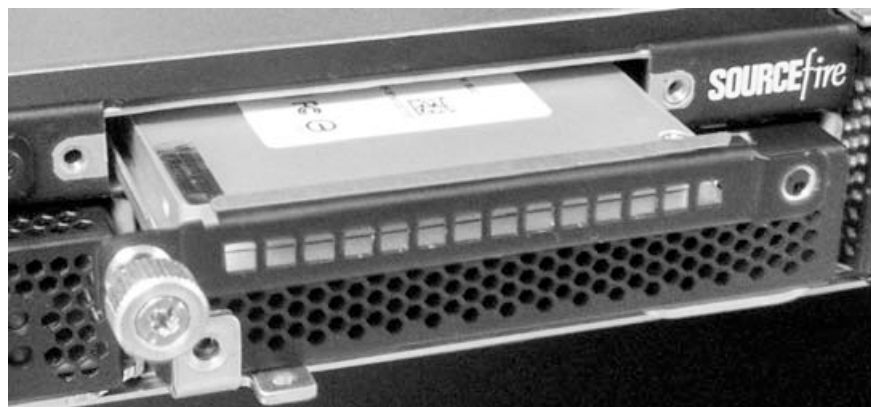

Step 4   Remove the malware storage pack from its packaging.

Step 5   Align the malware storage pack with the SSD bay and insert the malware storage pack into the device.

Step 6   Tighten the thumb screw on the malware storage pack to secure the storage pack into the device.

Step 7   Use the T8 Torx driver to replace the screw removed in Step 1.

Step 8   Turn on the system.

Refer to <Blue>Post Installation on page 11 for information on restarting a device after a malware storage pack has been installed.

# Instructions for the 82xx Family and 83xx Family Devices

The following sections describe how to install a malware storage pack SSD in the following 8000 Series devices with 2U chassis:

- 82xx Family devices (Firepower 8250, 8260, 8270, 8290)
- 83xx Family devices (Firepower 8350, 8360, 8370, 8390)

82xx Family Chassis Rear View

The SSD trays are located on the rear of the 82xx Family chassis.

Figure C-3   *82xx Family Rear View*
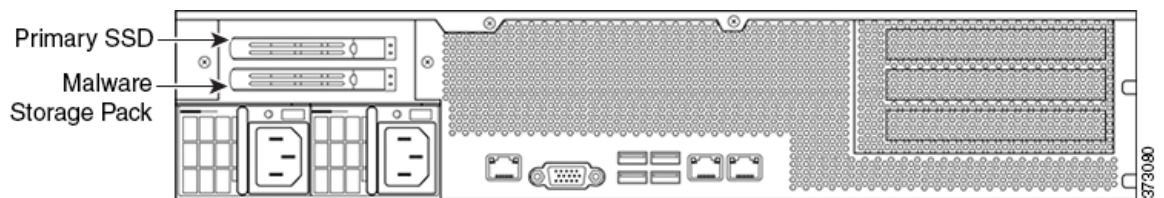
83xx Family Chassis Rear View

The SSD trays are located on the rear of the 83xx Family chassis.
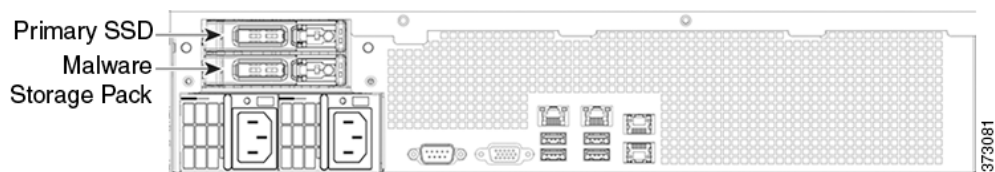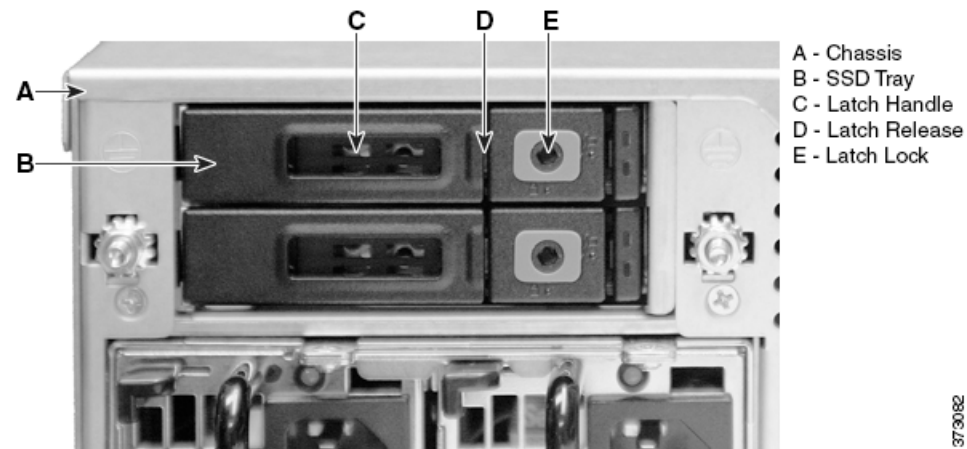
Figure C-4   *83xx Family Rear View*

Figure C-5   *SSD Detail*

A - Chassis
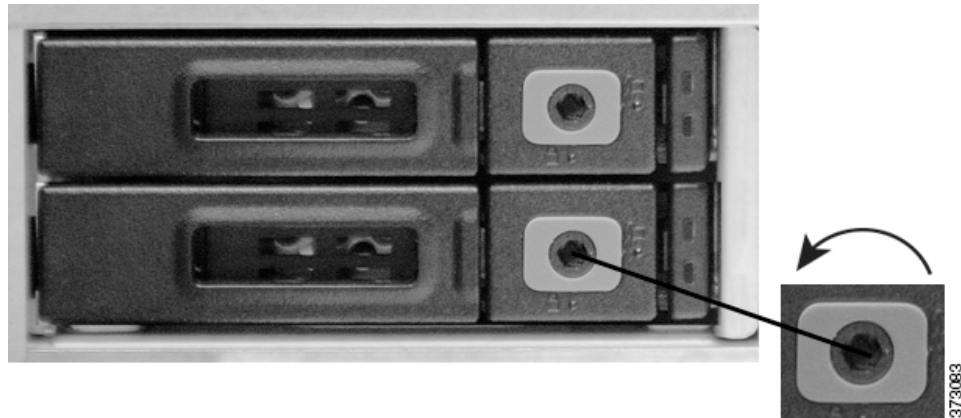B - SSD Tray
C - Latch Handle
D - Latch Release
E - Latch Lock

The following steps describe how to install a malware storage pack in the 82xx Family and the 83xx Family of devices. Install the malware storage pack in the SSD bay labeled *Malware Storage Pack*. Remove the empty SSD tray and replace it with the appropriate malware storage pack.

Note   Use proper electrostatic discharge (ESD) practices such as wrist straps and an ESD work surface.

Step 1   Ensure the device is powered off before you begin to install or remove a malware storage pack.

Step 2   Use the 3 mm hex wrench to unlock the latch release on the bottom SSD tray by turning the hex screw one quarter turn counter-clockwise, towards the unlock icon (   ).

Step 3   Press the latch lock to release the latch handle.
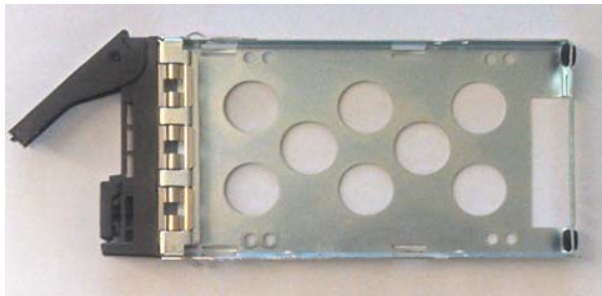
The latch handle opens toward you.
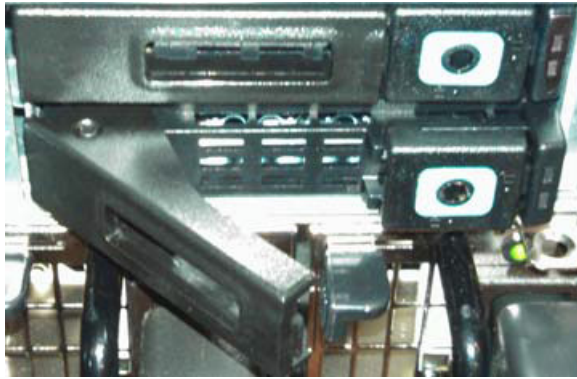
Step 4 Pull the latch handle to remove the SSD tray from the device.

✎

Note Retain the empty SSD tray. If you need to remove the malware storage pack at any time, re-install the empty tray in the device.

Step 5 Remove the malware storage pack from its packaging.

Step 6 Press the latch lock to release the latch handle.

The latch handle opens toward you.

✎

Note If the latch release is locked, use the 3 mm hex wrench to unlock the latch release on the malware storage pack by turning the hex screw one quarter turn counter-clockwise, towards the unlock icon (■).

Step 7   Align the malware storage pack with the SSD bay and insert the malware storage pack into the appliance.

Step 8   Push the latch handle on the SSD tray to secure the malware storage pack into the appliance.

Step 9   Use the 3 mm hex wrench to lock the latch release on the malware storage pack by turning the hex screw one quarter turn clockwise, towards the lock icon (█).
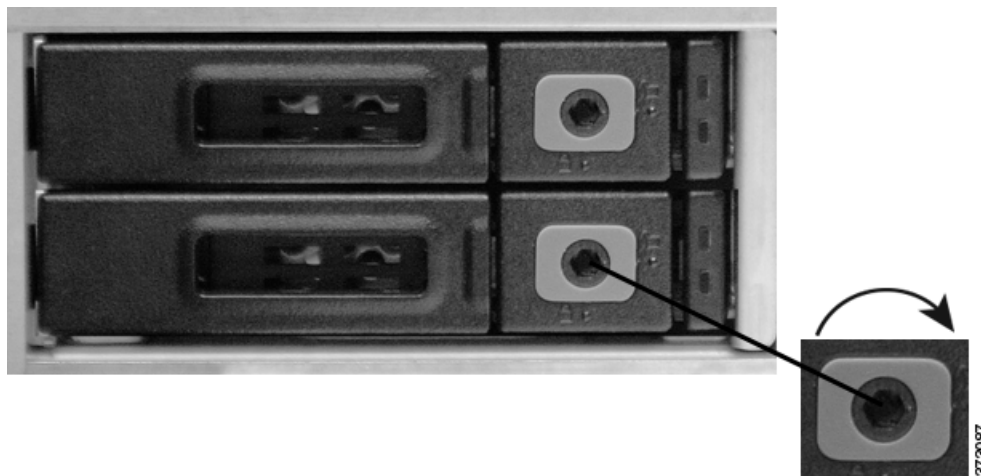
Step 10   Turn on the system.

Refer to <Blue>Post Installation on page 11 for information on restarting a device after a malware storage pack has been installed.

Post Installation

After installation of a malware storage pack is completed, you can restart the device to resume normal operation.

✎

Note   For information on how to safely restart or shut down the device, see the Managing Devices chapter in the *Firepower Management Center Configuration Guide*.

When you restart the device, the Firepower System automatically checks for the addition of the new storage pack. Before you restart the device, be aware of the following conditions:

- If a new (unformatted/unused) malware storage pack is detected, the Firepower System formats and mounts the disk for storage of suspected malware files and configures the malware storage pack with one partition that uses the entire drive space for file storage.

> **Note**   The Firepower System alerts you via a console message that the storage pack is being formatted. Depending on the storage capacity of the malware storage pack, formatting and configuration of a malware storage pack can take five or more minutes. Do not reboot or otherwise interrupt this process.

- If you add a malware storage pack to an 8000 Series device that has already been used to capture files on the primary SSD, the Firepower System moves the files stored on the primary SSD to the new malware storage pack in an effort to preserve the files and to recover space previously used on the primary SSD.

> **Note**   The Firepower System alerts you via a console warning message that file capture data is being transferred from the primary SSD. The file transfer process can take five or more minutes. Do not reboot or otherwise interrupt this process.

Note that you can remove a malware storage pack from a device at any time. A malware storage pack with file capture data can be relocated to another compatible device running Firepower System. Any file capture data on the primary drive will be transferred to the relocated malware storage pack, and any existing data on the malware storage pack from the previous device will remain intact in its original directory structure. Also, you can use the Firepower System to monitor the usage and health of a malware storage pack.

For more information, see:

- <Blue>Removing a Malware Storage Pack on page 12
- <Blue>Monitoring a Malware Storage Pack on page 13

Removing a Malware Storage Pack

You can remove a malware storage pack from a device and you can relocate a malware storage pack to another device.

To remove a malware storage pack from a device:

Step 1   Shut down the system.

Step 2   Power off the device.

Step 3   Remove the malware storage pack:

- For 81xx Family devices, refer to <Blue>Instructions for the 81xx Family Devices on page 5 (in reverse order).
- For 82xx Family and 83xx Family devices, refer to <Blue>Instructions for the 82xx Family and 83xx Family Devices on page 8 (in reverse order).

Step 4   Turn on the system.

Removing a malware storage pack will trigger a health alert. For more information, see the Using Health Monitoring chapter in the *Firepower Management Center Configuration Guide*.

Monitoring a Malware Storage Pack

Use the Firepower System to monitor your malware storage pack. The Firepower System provides information on usage, including the percentage of space used on the malware storage pack and the capacity of the malware storage pack. The Firepower System also provides many useful monitoring features to assist you in the daily administration of your system, including health modules. For more information, see the *Firepower Management Center Configuration Guide*.